UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE CIENCIAS Y SISTEMAS

MAESTRÍA EN GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

CICLO ACADÉMICO 2017- 2019

Tesis de Maestría

Propuesta de detección y mitigación de ataques de denegación de servicios en las redes institucionales DGI

Elaborada por:

Ing. Wilfredo Rodríguez Aburto #Carnet 2017-0011M

Ing. Pedro José Castellón Mena #Carnet 2017-0003M

Tutor: Msc. Yasser Membreño Gudiel

Managua, Nicaragua Noviembre del 2019

Tabla de contenido

I. INTRODUCCIÓN 1
II. ANTECEDENTES 2
III. JUSTIFICACIÓN 3
IV. OBJETIVOS 4
V. MARCO TEÓRICO 5
5.1 Fundamentación teórica 5
5.2 Categorías de ataques o amenazas. 5
5.3 El atacante 5
5.4 Ataques de Denegación de Servicios Distribuidos (DDoS) 6
5.5 Seguridad 7
5.6 Métodos de defensa contra ataques de negación de servicio. 9
5.7 ACL (Access Control List) 12
5.8 Objetivos de las ACL 12
5.9 Escenario real de la infraestructura de red de la Dirección General de Ingresos 13
5.10 Implementación del Gestor Unificado de Amenazas 13
5.10.1 Funciones y servicios que componen un gestor unificado y amenazas 14
5.10.2 Ventajas 15
5.10.3 Modo de implementarlo 16
5.10.4 Equilibrio de carga 17
5.11 Análisis comparativo de distintas soluciones UTM del mercado 19
5.12 Descripción de características de Sophos UTM 23
5.12.1 Los requerimientos de hardware para la instalación de Sophos UTM 24
5.12.2 Módulos que contiene SOPHOS UTM 24
5.12.2.1 Módulo Management 24
5.12.2.2 Módulo Definitions & Users 25
5.12.2.3 Módulo Interfaces & Routing 26
5.12.2.4 Módulo Network Services 26
5.12.2.5 Bind 27
5.12.2.6 Módulo Network Protection 27
5.12.2.7 Netfilter 28
5.12.2.8 Snort 28
5.12.2.9 Módulo Web Protection 29
5.12.2.10 Módulo Email Protection 29
5.12.2.11 Módulo Wireless Protection 30

5.12.2.12 Módulo Web Server Protection 30
5.12.2.13 Module Site-to-Site VPN 31
5.12.2.14 Módulo Remote Access 32
VI. DISEÑO METODOLÓGICO DE LA INVESTIGACIÓN 33
VII. ANÁLISIS DE MECANISMOS DE DETECCIÓN DE ATAQUES DDOS 34
7.1 Procesamiento de PVA 35
7.2 Arquitectura de proxy completo 35
7.3 Validación de protocolo 35
VIII. PLAN DE MITIGACIÓN DE ATAQUES DDOS 37
8.1 Pasos del plan de Mitigación de Ataques DDoS 37
IX. IMPLEMENTACIÓN DEL GESTOR UNIFICADO DE AMENAZAS (UTM) 34
9.1 Identificación de la infraestructura actual de la red institucional de la Dirección General de Ingresos (DGI) 35
9.2 Análisis de diferentes tecnologías firewall UTM 39
9.3 Análisis de firewall Fortinet UTM 41
9.3.1 Administración simple 44
9.3.2 Amplié rápido y fácilmente 44
9.3.3 Libere recursos 44
9.4 Análisis de Firewall UTM SOPHOS de última generación 44
9.4.1 Network Protection 46
9.4.2 Email Protection 46
9.4.3 Wireless Protection 46
9.4.4 Web Protection 47
9.4.5 Web Server Protection 47
9.4.6 Sandbox Protection 47
9.4.7 Sophos Red 48
9.4.8 Puntos de acceso Wi-Fi 48
9.4.9 Clientes VPN 48
9.4.10 UTM Manager gratuito 48
9.5 Mejoras en su conectividad 49
9.5.1 Segundo módulo Wi-Fi 49
9.6 Fuente de alimentación redundante 49
9.7 UTM que proporciona portal VPN 49
9.8 Expone riesgos ocultos 49
9.9 Bloquea amenazas desconocidas 49

9.9.1 Responde automáticamente a incidentes 50
9.10 Análisis de Firewall Check Point UTM 50
9.10.1 Características de Check Point UTM 51
9.11 Solución propuesta de implementación de un gestor unificado y amenazas de acuerdo a un análisis de las tecnologías. 53
9.11.1 Aspectos a considerar 54
9.12 Costos de implementación Sophos XG 210 55
9.12.1 Características técnicas de los servicios de seguridad requeridos. 57
9.12.2 Funcionalidades de Seguridad a implementar o activar en el UTM de Sophos XG 210. 58
9.12.3 Cómo proteger la red contra ataques DoS y DDoS utilizando Sophos XG Firewall 59
9.12.4 Protegiendo su red de un ataque DoS 59
9.12.5 Protegiendo su red de un ataque DDoS 60
9.12.6 Pasos para configurar una política en módulo IPS del UTMI. 61
9.12.7 Información Adicional 61
9.12.8 Flujo de muestra 61
9.13 Ventajas y desventajas de un UTM 62
9.14 Requerimientos de instalación y configuración 63
9.15 Diseño y arquitectura de la solución 64
9.16 Diseño lógico a Implementar 64
9.17 Perfiles de seguridad 65
9.18 Monitoreo de servidores 65
9.19 Resultado e impacto esperado 65
9.20 Impacto esperado 66
X. CONCLUSIONES 68
XI. RECOMENDACIONES 69
XII. BIBLIOGRAFIA 71
XIII. ANEXOS 75
13.1 Diagrama de funcionamiento de WAF para las redes internas de la DGI. 75
13.2 Reporte de ataques a la DGI. 76
13.3 Comparación de las características de seguridad independientes de los dispositivos UTM de las principales marcas 77
13.4 Proforma de UTM Fortinet 79
13.5 Oferta solución firewall 80
13.6 Oferta económica de proveedor 84

13.7 Implementación del proveedor 85
13.8 Oferta economica del proveedor 90
13.9 Características técnicas de Sophos UTM XG 210..... 91

I. INTRODUCCIÓN

La falta de seguridad es uno de los problemas más trascendentales que influyen en las redes y sistemas de comunicación, donde los ataques informáticos hacen uso de las vulnerabilidades en software y hardware incluso de sus componentes previamente conectados dando un efecto negativo en la seguridad de los mismos afectando a los activos que constituyen una organización.

Existen algunos tipos de ataques que son transmitidos en la red; entre los ataques más comunes estos: buffer overflow, shellcode backdoor, sniffing, keylogging, spoofing, trojan, denial of service, Distributed Denial of Service (DDoS) (Molina Lorena, 2015)(Armatte, 2016)(Biazus, 2016)(C. Rosales Garcia, 2011)(Cooke, 2014)(DK, 2013).

La Dirección General de Ingresos DGI, es una Institución descentralizada con autonomía administrativa y financiera, que regula los ingresos a favor del Estado. En la actualidad cuenta con servicios en línea que están de cara a los contribuyentes para realizar todas sus gestiones administrativas referente a la tributación nacional. Estas nuevas formas de recaudación ha llevado a la Dirección General de Ingresos que todas sus redes están expuesta a los ciberdelincuentes.

Desde el año 2016 fue punto de reflexión en la estrategia de seguridad para la Institución al revelarse el tamaño que pueden alcanzar los ataques distribuidos de denegación de servicio (DDoS) —tales como el ataque del código malicioso Mirai en octubre del 2016—, explotando las vulnerabilidades en dispositivos inteligentes y en otros dispositivos conectados a Internet. Detrás de las acciones del ataque de Mirai contra un proveedor de Internet en Estados Unidos y las del Ransomware llamado WannaCry en el año 2017, actividades como estas de los ciberdelincuentes se incrementan a diario. La DGI es vulnerable a estos ataques debido a la falta de equipos de seguridad para poder mitigarlos en la Institución, por lo que con esta propuesta que se está diseñando en este proyecto de tecnología basado en la protección de todas las redes internas de la institución.

II. ANTECEDENTES

En un reporte del periódico el Nuevo diario el 15 de Septiembre del 2011 un ataque masivo por hacker de conocidos como anonymous dejó sin acceso a los sitios web al menos 10 instituciones gubernamentales.

En el caso de la DGI en los últimos 5 años se ha fortalecido la seguridad ante los ataques de DDoS por medio de la adquisición de dispositivos de seguridad como los ASA Cisco que son una plataforma que proporciona servicio de seguridad a las VPN, protege los servidores y la infraestructura contra gusanos, piratas informáticos y otras amenazas mediante una combinación de servicios de firewall, seguridad de aplicaciones y prevención de intrusiones. La DGI tiene un ancho de banda disponible por parte del proveedor para Internet de 30 Mbps.

En este último año se adquirió Web Application Servicies para proteger todos los servicios web que brinda la Institución hacia los contribuyentes, Pero en la actualidad con esta tecnología la DGI no está protegida completamente por que a diario hay ataques hacia las redes, donde el atacante está buscando la puerta de acceso y vulnerabilidades para penetrar.

La tecnología avanza día a día para hacernos la vida más fácil. Sin embargo, también los ciberdelincuentes se las ingenian para aprovecharse de aquellas personas e instituciones que no siguen las recomendaciones de seguridad y por lo tanto se convierten en presa fácil para sus ataques.

Uno de los más sonados en la web son “los ataques distribuidos de denegación de servicio”, conocidos como DDoS por sus siglas en Inglés (Feintein. L, 2013)(Garcia, 2010) Distributed denial of service attack). Esta es una técnica usada por hackers en la que, usando redes de bonets y software malicioso instalado en miles y miles de máquinas, se generan tantas solicitudes al servidor de un sitio web que éste termina por caerse.

Ese es el objetivo de los ataques DDoS: que los usuarios reales de un sitio web no puedan ingresar porque el servidor no da abasto para tantas solicitudes de información.

III. JUSTIFICACIÓN

Este proyecto es importante, ya que analizará las vulnerabilidades en el estándar de las redes externas e internas. El principal beneficiario de este proyecto sería: La Dirección General de Ingresos.

Al implementar esta plataforma de seguridad, la institución tendrá los beneficios de proteger la red interna de accesos no autorizados que se puede intentar en una red de área local (LAN) o Internet y con la intención de explotar vulnerabilidades en los sistemas de la red interna. Con los firewalls puede "ocultar" la identidad de los equipos como medio de prevención ante los intentos de escaneo o intrusión a las computadoras por los hackers.

La seguridad es una de las principales preocupaciones que tiene la institución, cuando la red privada se conecta hacia Internet. Para conseguir un nivel de protección aceptable, será necesario políticas de seguridad para evitar que usuarios sin autorización tengan acceso a los recursos de la red privada y protegerla contra la exportación sin autorización de la información confidencial de la institución.

Una vez implementado este firewall será como un cuello de botella por el que todo el tráfico de Internet entrante y saliente debe pasar, permitiendo controlar el tráfico. Con este cortafuegos bien configurado y administrado evitará en gran medida que los hackers accedan con facilidad y por supuesto ayudara a mantener a salvo los datos confidenciales de la institución. Este firewall trabaja como un policía identificando cada paquete de información antes de que este le permita el acceso como:

- Monitoreo y registro de los servicios utilizados para usar Internet, FTP y otros protocolos.
- Permitirá definir una "barrera" manteniendo a un lado a los usuarios sin autorización.
- Prevención de los ataques hacia tu red privada desde otras redes externas.
- Control de la seguridad en la red y los equipos individualmente cuando se produzca cualquier actividad sospechosa.
- Control del uso de Internet bloqueando o desbloqueando material inapropiado o apropiado.

IV. OBJETIVOS

OBJETIVO GENERAL

- Propuesta de detección y mitigación de ataques de denegación de servicios en las redes institucionales DGI.

OBJETIVOS ESPECÍFICOS

- Analizar los ataques de DDoS en los servidores de nombres de dominios y los mecanismos de detección.
- Implementar en la infraestructura de red de la Dirección General de Ingresos un plan de mitigación de los ataque DDoS.
- Implementar un gestor unificado de amenazas para contrarrestar los ataques que sufre la institución.

V. MARCO TEÓRICO

5.1 Fundamentación teórica

Tomando en consideración el conocimiento sobre lo que sucede en la actualidad sobre los ataques DDoS y mecanismos de detección entre otros, se contextualiza lo siguiente:

¿Qué es un ataque?

Según (Narvaez D. R., 2010) un ataque a la seguridad de red produce un acceso no autorizado, denegando el sistema a través de estas anomalías que acechan en la actualidad, por lo que existen diversas categorías de ataques o amenazas.

5.2 Categorías de ataques o amenazas.

- Ataques por interrupción: Un elemento del sistema es eliminado o se vuelve inutilizado, este tipo de ataque es en contra de la disponibilidad.
- Ataques por intercepción: Cuando un individuo consigue acceso al sistema de manera no autorizada, este tipo de ataque es considerado contra la confidencialidad.
- Ataques por modificación: Cuando un individuo consigue asistir al sistema no sólo de manera no autorizada, sino que puede alterarlo dando así el tipo de ataque contra la integridad.
- Ataques por Falsificación (Phishing): Cuando un individuo accede de manera no autorizada e ingresa objetos falsificados dentro del sistema, generando el ataque contra la autenticidad.

5.3 El atacante

El atacante es aquella persona que detecta los puntos más vulnerables de la red y que permiten el acceso al sistema con la finalidad de inundar de paquetes a un determinado servicio a través de una gran cantidad de máquinas (Zombies). Esto tiene como consecuencia el rendimiento pausado, hasta que el servicio quede inutilizado por un determinado tiempo causando incluso grandes pérdidas económicas en la organización(Hoque.N, 2016).

5.4 Ataques de Denegación de Servicios Distribuidos (DDoS)

Esta técnica de ataque apareció por primera vez en junio de 1998 y actualmente es la técnica más eficiente y difícil de detectar por su naturaleza distribuida.
La Denegación de Servicio Distribuido (DDoS) es considerado un ataque peligroso que infecta de gran cantidad de peticiones ficticias a un determinado servicio de la red. Con esto logra que el servicio se detenga, generando una sobrecarga en la utilización del mismo y por lo tanto, un incremento exponencial de anomalías (J. Mirkovic, 2014)(J.Arzamendia, 2016).

Figura 1. Arquitectura de un ataque DDoS (Molina Lorena, 2015).

Los ataques DDoS son los más frecuentes y aumentan a diario debido al inmenso desarrollo de redes informáticas y en conjunto a varias aplicaciones que causan daño a las redes y sistemas de información. Por ejemplo, los botnets son una amenaza crítica que tienen como consecuencia disminuir el ancho de banda y los recursos de los sistemas (Hoque. N, 2015)
Los ataques DDoS pueden ser clasificados de acuerdo a su dimensión. Los ataques basados en la taxonomía se clasifican en: grado de automatización, exploración de vulnerabilidades, tasa de ataque dinámico y según su impacto (Lau, 2012).

Un tipo de ataque según dicha clasificación es UDP Flood. Un ataque de esta naturaleza es posible cuando el atacante envía un gran volumen de paquetes IP con datagramas UDP a un puerto aleatorio de la víctima. El envío excesivo de datagramas UDP puede producir la caída

del sistema. La víctima podría ser un servidor de nombres de dominio (DNS) que es un sistema distribuido jerárquico cuya función es traducir las direcciones IP en etiquetas de servicio de red. DNS utiliza una base de datos distribuida y jerárquica que almacena información asociada a nombres de dominio en redes como Internet. Este protocolo está definido en RFC 1034 y en el RFC 1035 usa UDP como protocolo de capa transporte y trabaja en el puerto 53 por defecto (Saravanan, 2012).

Otro tipo de ataque muy conocido es SYN Flooding. Uno de los ataques DDoS que aparecieron por primera vez y ahora el más utilizado es: La inundación SYN funciona aprovechando las debilidades del protocolo de control de transmisión (TCP). La figura 1 muestra el mecanismo del ataque de inundación SYN. El paquete SYN es un tipo de paquete en el Protocolo de Control de Transmisión (TCP) que requiere establecer una conexión entre dos hosts. Es una solicitud enviada por el host para hacer una conexión.

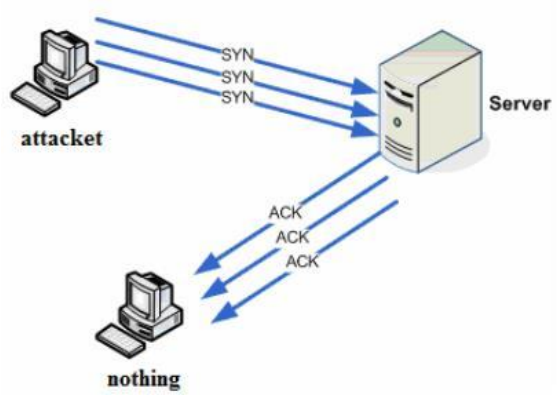


Figura 2. Mecanismo SYN Flooding (Sanmorino, 2013).

5.5 Seguridad

La seguridad en la red se ha convertido en un esfuerzo sumamente importante y que presenta grandes desafíos para las organizaciones hoy en día. La finalidad es proteger la información confidencial e importante para brindar un servicio sin interrupciones evitando que diversas anomalías causen que los servicios se detengan (DK, 2013).

Para garantizar la implementación de los diferentes servicios de seguridad existen tres campos de trabajo que deben ser considerados:

Prevención: Para proporcionar un primer nivel de seguridad, es necesario prevenir los ataques a la seguridad del sistema que debe ser protegido.

Detección: Una vez que las medidas preventivas se han implementado, hay que considerar que un atacante puede evitar dichas medidas. Será necesario, por tanto, disponer de un método que permita detectar las violaciones de la política de seguridad que se produzcan en el sistema. Respuesta: Las organizaciones y necesitan desarrollar un plan que establezca las respuestas concretas a ejecutar ante determinadas violaciones de la política de seguridad.

Por otro lado, para definir e implementar los servicios necesarios para garantizar que un sistema se considere seguro, se utilizan diferentes modelos [Canavan, 2001] que determinan la arquitectura de la red y la configuración de los sistemas. En general, la utilización de un modelo no excluye la incorporación de aspectos de otro, de modo que la mayoría de los sistemas de seguridad incorporan características o variantes procedentes de alguno de estos modelos:

- Seguridad por oscuridad: Este modelo se basa en el concepto de que, si una entidad no conoce la existencia de una red o sistema, no intentara atacarlo. Supone que la ocultación de un elemento en la red constituye un nivel de seguridad suficiente.

- La defensa perimetral: Este tipo de defensa es análoga a la ofrecida por una muralla que protege un castillo. Las empresas y corporaciones que utilizan este modelo de seguridad fortalecen sus sistemas perimetrales y encaminadores de salida. Un ejemplo de implementación de este modelo son los sistemas denominados cortafuegos [Goncalves, 1997], que separan los sistemas a proteger del exterior considerado no seguro.

- La defensa en profundidad: Esta es la aproximación más robusta. Persigue establecer un sistema seguro mediante la monitorización y fortalecimiento de todos los elementos que conforman la red y no solamente del perímetro como en la aproximación anterior.

Aunque en dicho perímetro las medidas deben ser más robustas y con funcionalidades más avanzadas, la seguridad de los elementos interiores no dependerá exclusivamente de la aplicada en el perímetro, sino que tendrá que ser reforzada con nuevos elementos. Este paradigma es más difícil de implementar y requiere que todos los elementos interiores y sus administradores se involucren en la puesta en práctica de las políticas de seguridad.

5.6 Métodos de defensa contra ataques de negación de servicio.

Las maniobras de prevención tienen el propósito de intentar eliminar la posibilidad de que un ataque se realice antes de que este se lleve a cabo de manera real. Estos acercamientos permiten implantar cambios en los protocolos, aplicaciones y sistemas para robustecerlos contra los intentos de ataque. La prevención, referida a los ataques DDoS, tiene como objetivo disminuir el riesgo de sufrir algunos de los ataques de vulnerabilidad, además de dificultar al atacante la tarea de conseguir una cantidad de agentes elevados y reduce las probabilidades de éxito del ataque. Pero, aunque la prevención juega un papel primordial para la seguridad, de ninguna manera elimina la amenaza que suponen los ataques de denegación de servicio. En el campo de la prevención de ataques DDoS, se podrían clasificar las posibles medidas en cuatro grandes grupos:

Mecanismos de seguridad del sistema: Son mecanismos que tratan de incrementar la seguridad global del sistema, mediante la defensa contra accesos ilegítimos, eliminando bugs en las aplicaciones, actualizando las implementaciones de los protocolos para evitar intrusiones y la utilización del sistema con fines delictivos.

Mecanismos de seguridad en protocolos: Son aquellos que abordan el problema de un diseño defectuoso en los protocolos de comunicaciones.

Mecanismos de supervisión de recursos: Son aquellos que controlan el acceso de cada usuario a los recursos, fundamentándose en los privilegios que posee dicho usuario y en su conducta. Estos mecanismos garantizan un servicio adecuado a los usuarios legítimos, a la vez que

deniegan el acceso a los que no tienen permiso. Obviamente, con el objetivo de evitar el robo de identidad, prácticamente todas estas medidas se utilizan conjuntamente con mecanismos para verificar la identidad de los usuarios, es decir, con métodos de autentificación.

Mecanismos de multiplicación de recursos: Son aquellos que pretenden dotar de abundantes recursos a los sistemas para debilitar la amenaza que supone el agotamiento de los mismos por parte de un posible ataque DDoS. La aproximación más común consiste en contratar un ancho de banda elevado y desplegar un número más o menos elevado de servidores detrás de un balanceador de carga. Los servidores pueden compartir la carga de igual modo a cualquier hora, o bien se pueden dividir en servidores principales y de respaldo, los cuales se activarán cuando las máquinas principales no pueden procesar toda la carga.

Según (Javier Sanchez Gonzales, 2016), cuando un ataque DDoS no es masivo, una oportuna configuración del sistema operativo puede ser de utilidad para minimizar el ataque y habilitar nuevamente los servicios afectados. Los servidores emplean el sistema operativo Linux, por lo tanto, se investigara sobre los parámetros del kernel de Linux que ayudan a minimizar los ataques maliciosos como un mecanismo de defensa. Entre ellos, se pretende analizar los siguientes:

- Tcp_syncookies: Protege de los ataques Syn_Flood; dependiendo del kernel, responde un segmento syn-ack creando una serie de números codificados que representa la IP origen y destino, el puerto y el timestamp de la petición recibida. Comando de inicio de las cookies: sysctl-w net.ipv4.tcp_syncookies=1(Javier Sanchez Gonzales, 2016).
- Ignore Broadcasts: Protege de los ataques Smurf, envía paquetes ICMP a una dirección IP Broadcast de una dirección IP imitada inundando el servidor con el ataque Smurf; por lo tanto, para contrarrestar dicho ataque, se ejecuta el siguiente comando: sysctl-w net.ipv4.icmp_echo_ignore_broadcasts=1 (Javier Sanchez Gonzales, 2016).

- Rp_filter: Es la comprobación de los paquetes que acceden a una interfaz, basándose en una dirección original identificando así el ataque IP Spoofing: sysctl -w net.ipv4.conf.all.rp_filter=1 (Javier Sanchez Gonzales, 2016).

Una de las opciones para enfrentar los ataques DDoS es mediante la implementación de modelos de seguridad que utilizando diversas técnicas tanto para identificar las diversas anomalías que concurren en la red como para salvaguardar los servicios ofrecidos de un sistema. Esta da como resultado una disminución del tráfico de peticiones en el servidor.

Según (C. Rosales Garcia, 2011), la metodología impartida para la detección de ataques maliciosos es denominada red bayesiana, que permite identificar incidencias, de los ataques en la red de datos, como principio importante menciona que los investigadores forenses optan por herramientas que ayudan a identificar la información para el análisis el cual tiene como resultado minimizar los ataques y realizar un análisis forense con el objetivo de conocer la forma de trabajo del atacante y sus técnicas. Se define los procesos a seguir en el diseño de la red bayesiana: Identificación de ataques DDoS, Diseño de red Bayesiana, recolección de tráfico de red, filtrado de tráfico de red, pruebas de la metodología bayesiana, Ajustes al modelo de la red Bayesiana, Generación inferencial y Obtención de métricas finales.

Esta metodología fue diseñada principalmente para la obtención del tráfico de datos en la red, permitiendo eliminar en tiempo real los ataques DDoS, siendo los ataques con mayor incidencia en Internet.

A continuación, se presenta la funcionalidad de la red Bayesiana:

- Identificación del ataque DDoS.
- Emite un pronóstico al mismo.
- Envía alertas que determinan la incidencia detectada en la red.
- Emite una probabilidad de ocurrencia con un intervalo de confianza del 95 %.

5.7 ACL (Access Control List)

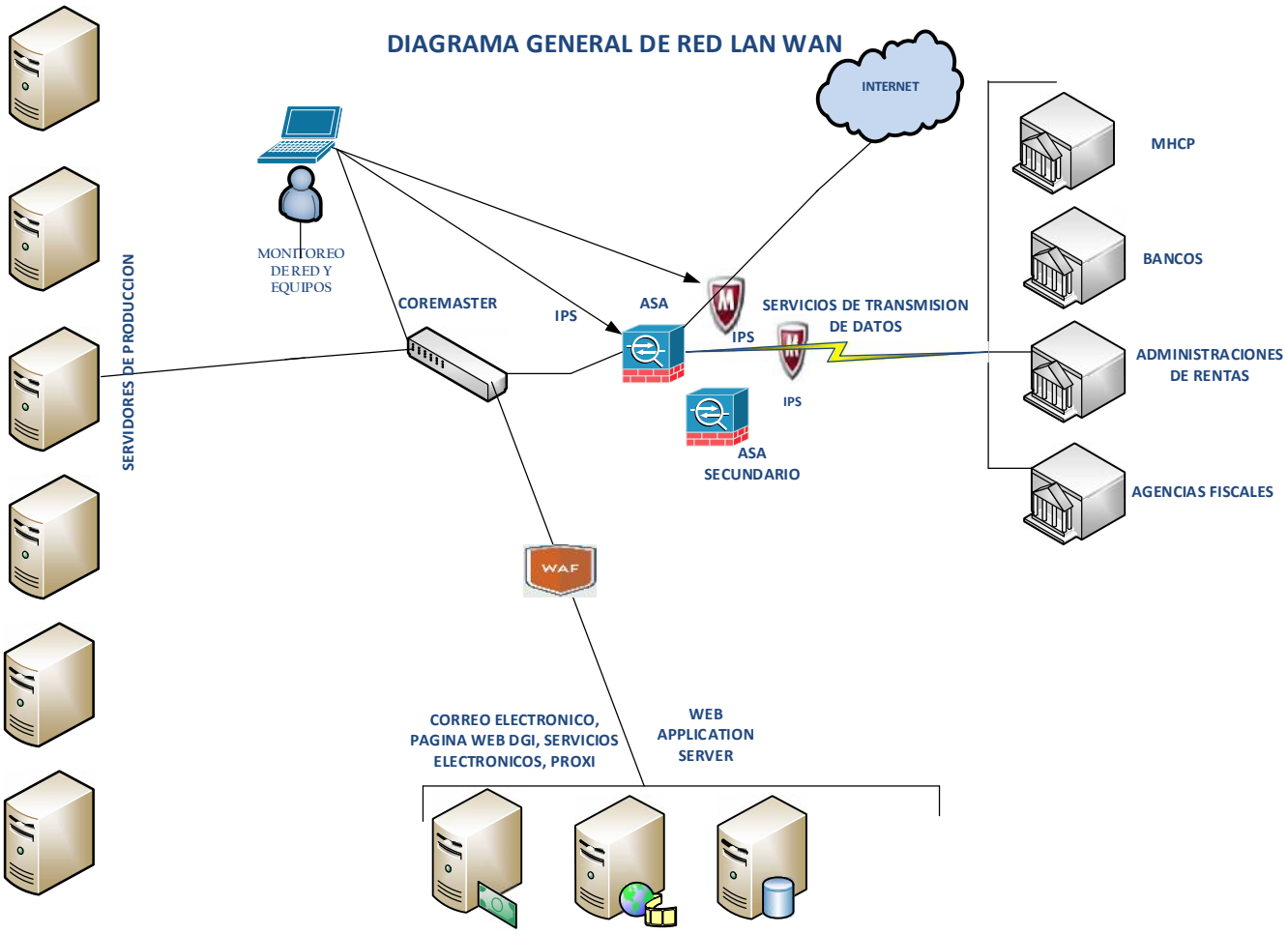
Según (Mifsud, 2015), ACL es un concepto de seguridad informática usado para fomentar la separación de privilegios. Es una forma de determinar los permisos de acceso apropiados a un determinado objeto, dependiendo de ciertos aspectos del proceso que hace el pedido.
Las ACL permiten controlar el flujo del tráfico en equipos de redes, tales como routers y switches. Su principal objetivo es filtrar tráfico, permitiendo o denegando el tráfico de red de acuerdo con alguna condición. Sin embargo, también tienen usos adicionales, como, por ejemplo, distinguir “tráfico interesante" (tráfico suficientemente importante como para activar o mantener una conexión) en ISDN.

5.8 Objetivos de las ACL

Los objetivos que se persiguen con la creación de ACL son:

- Limitar el tráfico de red y mejorar el rendimiento de la red. Al restringir el tráfico de vídeo, por ejemplo, las ACL pueden reducir ampliamente la carga de la red y en consecuencia mejorar el rendimiento de la misma.
- Controlar el flujo del tráfico. Las ACL pueden restringir el envío de las actualizaciones de enrutamiento. Si no se necesitan actualizaciones debido a las condiciones de la red, se preserva el ancho de banda.
- Proporcionar un nivel básico de seguridad para el acceso a la red. Las ACL pueden permitir que un host acceda a una parte de la red y evitar que otro acceda a la misma área. Por ejemplo, el host-1 se le permite el acceso a la red de producción, y al host-2 se le niega el acceso a esa red.
- Establecer qué tipo de tráfico se envía o se bloquea en las interfaces del router. Por ejemplo, permitir que se envíe el tráfico relativo al correo electrónico y se bloquea el tráfico de ftp.
- Otorgar o denegar permiso a los usuarios para acceder a ciertos tipos de archivos, tales como FTP o HTTP.

5.9 Escenario real de la infraestructura de red de la Dirección General de Ingresos



5.10 Implementación del Gestor Unificado de Amenazas

El término gestor unificado de amenazas o UTM por sus siglas en inglés Unified Threat Management hoy en día se está empezando dar a conocer como un factor importante dentro del campo de la seguridad perimetral de redes.

El UTM puede definir la consolidación de distintas soluciones de seguridad de redes en una única solución ya sea esta de software o de hardware. La integración de estas soluciones incluye servicios como firewall, filtrado de contenido web, antivirus de puerta de enlace,

prevención y detección de intrusiones, acceso remoto a través de redes privadas virtuales o VPN *(*Virtual Private Network*),* usados para contrarrestar los más variados ataques de seguridad informática que sufren las organizaciones. Además, permite el balanceo de carga de enlaces de Internet lo cual se refleja en la continuidad de negocio.

5.10.1 Funciones y servicios que componen un gestor unificado y amenazas

Para comprender mejor a los gestores unificados de amenazas de red, se describe a continuación varios de los componentes de los mismos, dentro de ellos se encuentran tanto los componentes básicos como los avanzados, aclarando que los componentes básicos se encontraran siempre en cualquier gestor unificado de amenazas, y los componentes avanzados se encuentran en algunos, de acuerdo al fabricante que los produzca:

- Bloqueo y filtrado de contenido web tales redes sociales, paginas porno, juegos en línea, descargas de programas etc.
- Bloqueo de puertos con los cuales interactúan programas de mensajería como Messenger, AOL, Yahoo! Messenger y programas P2P como Emule, Ares, Etorrent ya que estos programas al ser de intercambio de archivos son punto de entrada para un potencial atacante.
- Bloqueo de archivos o extensiones como Js, Vb, Rar, Jar, Doc, Xls, mpg etc. y demás formatos multimedia ya que dentro de estas extensiones se pueden albergar programas como troyanos o rookits y otros tipos de malware
- Monitoreo de páginas web de almacenamiento en línea o de disco duros virtuales, de archivos adjuntos en emails, sistemas de mensajería instantánea ya que dentro de esos archivos también se podría algún albergar tipo de malware
- Protección de malwares y sypwares, etc. integrando dentro de su plataforma aplicativos para combatir estas amenazas ejemplos: antivirus, antispyware entre otros.
- Protección frente a ataques de negación de servicios y de negación de servicios distribuidos y de escaneo remoto no autorizado de puertos, bloqueando los respectivos puertos vulnerables.

- Protección de correo no deseado mediante aplicación de reglas para la recepción y envío de mensajes masivos con contenido ofensivo o fraudulento.
- Controla el ancho de banda regulando la carga y descarga de archivos, la tasa de trasferencia por equipos al acceder a la web, implementando políticas de control de ancho de banda demandada por sitio, contenido y protocolo.
- Permite crear redes DMZ definiendo la segmentación de las redes a proteger configurándolas por zonas, también está integrado en un UTM el servidor proxy el cual optimiza el ancho de banda cuando se guarda una cache de contenido, garantizando también una navegación anónima
- También permite crear redes privadas mediante la técnica de tunneling facilitando el acceso remoto a los recursos de los sistemas empresariales, también integra aplicativos de seguridad que tiene características de autentificación como LDAP, directorio activo o Radius.
- La última pero no menos importante es que muestra reportes detallados de eventos como: uso de ancho de banda, graficas de rendimiento de la red, malwares detectados, uso de servicios de red y correo interno, todo esto en tiempo real mediante reportes centralizados de la red.- Autenticación de doble factor.
  - Protección contra amenazas avanzadas.

5.10.2 Ventajas

Las ventajas más importantes serian: Fácil administración ya que se ejecutan de una manera centralizada, servicios integrados por diversos aplicativos como:

IPS/IDS (sistemas de detección de intrusos, sistemas de prevención de intrusos), VPN IPsec y SSL, Antivirus, AntiSpyware, Firewall, AntiSpam y Filtro de contenidos dando máxima seguridad algunas de estas funcionalidades.

Sus ventajas pueden compensar fácilmente sus inconvenientes, pero según los expertos, no es recomendable contar con un único punto de mitigación de riesgos a través del cual fluya todo

el tráfico cuando la red cuenta con docenas, cientos o miles de localizaciones; y por varias razones. Hay responsables de TI que son reacios a poner todas sus herramientas de seguridad en un mismo punto, por cuanto tales despliegues suponen un único punto de fallo. No obstante, se puede soslayar este inconveniente instalando UTM en forma redundante con propósitos de failover, lo que ofrece mayores niveles de disponibilidad.

Además, como en las redes de gran tamaño la capacidad de proceso real es una cuestión crítica, los responsables de TI a menudo prefieren distribuir la protección contra retos en vez de centralizarla, simplemente para reducir la probabilidad de que se produzca un cuello de botella del rendimiento» (Network World, 2010).

5.10.3 Modo de implementarlo

Las implementación de un UTM a 3 capas garantizando seguridad en las terminales de trabajo servidores de procesamiento de datos y acceso a internet , por ejemplo al configurar los firewalls del UTM se debe configurar de tal forma que filtren paquetes de datos , funcione la puerta de enlace nivel de aplicación y la puerta de enlace nivel de circuitos o cuando se configuren los routers por medio del UTM, estos deben filtrar la información en los niveles de red y transporte (protocolos IP, TCP, UDP, ICMP), inspeccionar la información contenida en cada paquete recibido o enviado , comprobar que estos paquetes de datos cumplen las reglas o criterios de filtrado según las listas de control de acceso y ejecutar las políticas por defecto como : discard/deny y forward/allow o para una protección más avanzada usar también los servidores proxy integrado en los UTM o también llamados Gateway a nivel de aplicación los cuales , conmutan el tráfico a nivel de aplicación , controla contenidos , intercepta mensajes entre aplicaciones bloqueando aplicaciones no permitidas (sin proxy), también detectando uso de protocolos no permitidos en puertos estándar. Esto con el fin de conectar la organización al internet y evitar posibles daños a la información.

Para Fortinet (2009), independiente de la clasificación anterior, la tecnología UTM busca:

- Minimizar los riesgos de seguridad en los negocios.
- Reducir la sobrecarga de trabajo en la administración de la seguridad de las organizaciones y dar un uso más eficiente al personal interno.

- Mejorar la infraestructura de seguridad existente.
- Aumentar los niveles de cobertura en la gestión y administración de la seguridad.
- Minimizar los gastos de múltiples dispositivos y a la vez maximizar la protección.
- Acelerar la resolución de incidentes sin la necesidad de contar con personal.
- Centralizar la administración.
- Facilidad de mantener una política global y coherente a dispositivos de seguridad.
- Monitoreo y registró en tiempo real de todo lo ocurrido.

El diferenciador clave para determinar que un dispositivo realiza UTM es tener la capacidad de inspeccionar y determinar si los paquetes de datos que analiza, individuales o múltiples, son una amenaza, en otras palabras, debe proporcionar una inspección profunda de paquetes a través de escaneos internos.

5.10.4 Equilibrio de carga

Los productos UTM de alta gama permiten a los administradores de seguridad en las redes de las organizaciones, utilizar todos los servicios ofrecidos con un gran rendimiento ya que utilizan lo que se conoce como equilibrio de cargas UTM.

Según SonicWall (2009), el equilibrio de carga como se puede apreciar en su estructura en la figura 1, cuenta con un motor de inspección de paquetes y de clasificación de datos que a una alta velocidad y a través de distintos núcleos de seguridad permite inspeccionar en tiempo real aplicaciones, archivos y tráfico sin que esto repercuta en el rendimiento.

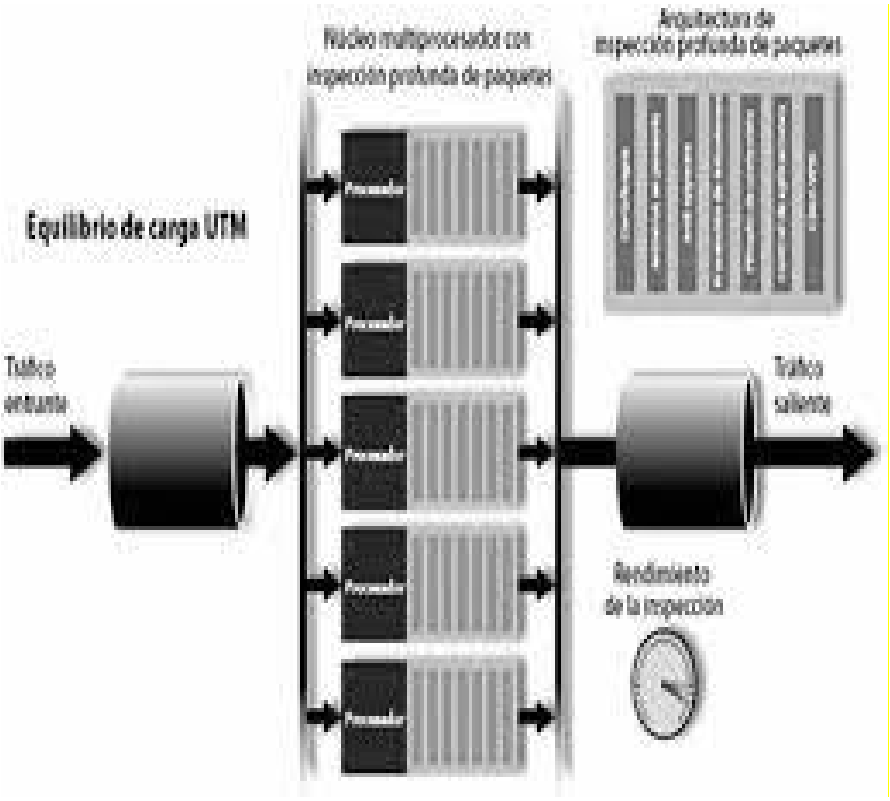


Figura 1. UTM – estructura interna en el equilibrio de carga (Sonicwall, 2009)

El mecanismo, es la base para que esta herramienta pueda soportar todo el tráfico entrante y saliente, además de eso determinar a través de las distintas aplicaciones, cual es el tratamiento que se le debe dar a los datos y los recursos que requiere para que sea conducido por el canal correcto sin pérdida de información y con la rapidez suficiente.

Los cortafuegos UTM son especialmente atractivos cuando el rendimiento es un factor clave, ya que permiten escalar mediante actualizaciones sencillas, añadiendo mejoras en el chasis o sistemas en una configuración de balanceo de cargas activo/activo. Pero es mejor comenzar con un sistema que corra tan rápido como precise nuestra red y darse un tiempo hasta la próxima actualización (Network World, 2010

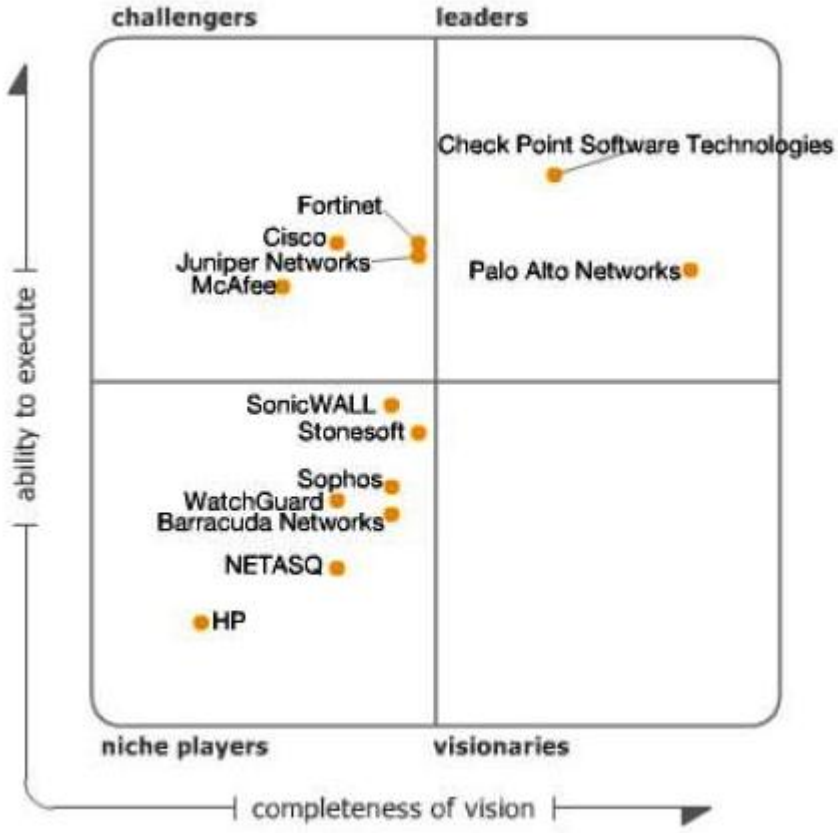
5.11 Análisis comparativo de distintas soluciones UTM del mercado

Para seleccionar el UTM ideal y que cubra las necesidades de protección de la Institución se realizó un análisis de 5 soluciones UTM disponibles en el mercado, siendo las siguientes; Sophos UTM, Zentyal Gateway & UTM, Fortigate, SonicWall y Handec.

CUADRO N° 1: Comparativo de soluciones UTM en el Mercado.

https://www.sophos.com/en-us/lp/xg-firewall.aspx

Características	Zentyal Gateway & UTM	Sophos	Fortigate	SonicWall	Handec
Firewall	si	si	si	si	si
IPS	si	si	si	si	si
VPN	si	si	si	si	si
Filtrado de Navegación	si	si	si	si	si
QoS	si	si	si	si	si
Protección Antivirus	no	si	no	no	si
Firewall de aplicaciones	no	si	no	no	si
Portal de Usuario	no	si	no	no	si
Reporteria completa	condicionado	si	condicionado	condicionado	condicionado
Factor de doble autenticación integrado	no	si	no	no	si
Protección contra amenazas avanzadas	no	si	no	no	si
Control de aplicaciones	si	si	si	si	si
Versión software	si	si	si	si	si
Versión libre	si	no	no	no	si



https://www.computing.es/seguridad/informes/1037053002501/gartner-cuadrante-magico-firewalls.1.html

CUADRO N° 2

Gartner ha publicado su Cuadrante Mágico sobre el mercado de los proveedores más importantes de firewalls. Ha reconocido como líderes tan sólo a Check Point Software Technologies y Palo Alto Networks.(esecurityplanet, 2019)

Gartner ha publicado su Cuadrante Mágico sobre soluciones firewall para redes corporativas, que incluye una combinación de firmas grandes y medianas, con el elemento común de que fabrican productos creados a la medida de las necesidades de las organizaciones. Estas necesidades incluyen un amplio rango de modelos y soportes para la virtualización y la creación de redes LAN virtuales, así como una gran capacidad de gestión y reporting diseñada para entornos complejos con un alto volumen de información, incluyendo prestaciones de administración multi-capa y gestión avanzada de reglas y políticas.

Un elemento clave de estas soluciones es el concepto de "firewall de nueva generación" (NGFW, por sus siglas en Inglés), que toma sentido a medida que las organizaciones van abandonando el modelo tradicional de contar con dispositivos de seguridad sólo en su perímetro y en sus localizaciones remotas. Los fabricantes incluidos en este cuadrante lideran el mercado ofreciendo nuevas prestaciones que superan este modelo, con modelos avanzados que ya no tratan el firewall simplemente como un producto (commodity), sino como un elemento crítico del negocio, y cuentan con un buen historial en la neutralización de vulnerabilidades en sus productos de seguridad. Con estos criterios, Gartner ha reconocido como Líderes de este mercado tan sólo a Check Point Software Technologies y Palo Alto Networks. En el área de Challengers ha identificado a Fortinet, Cisco, Juniper Networks, y McAfee. En el campo de Jugadores de Nicho, ha ubicado a SonicWALL, Stonesoft, Sophos, WachtGuard, Barracuda Networks, Netasq y HP. En Visionarios no figura ningún proveedor.(esecurityplanet, 2019).

Handec Según (Sufian Hameed, 2016), menciona que el marco de detección de ataques DDoS en tiempo real obtenido por Hadoop (HADEC) posee cuatro fases importantes que son: Captura de tráfico de red, generación de registros, transferencia de registros, detección de DDoS, notificación de resultados, captura de tráfico de red y generación de registros.

En la detección de los ataques DDoS, HADEC proporciona una interfaz online que a través de la cual el administrador puede manipular el servidor con los parámetros según sea posible mantener una seguridad estable dentro de la entidad, el número de archivos a capturar antes de iniciar la fase de detección y la ruta en la cual se va a guardar el archivo capturado, luego de que el administrador realice las configuraciones necesarias, el tráfico de Handdle inicia con la detección de tráfico de paquetes en tiempo real (Sufian Hameed, 2016).

HADEC utiliza un componente Tshark que permite realizar dicha captura, se ha desarrollado la utilidad de java based (Echo Class) que permite el desarrollo de una conexión con Tshark para que a través de ella pueda leer paquetes de salida de Tshark puestas en un archivo de registro. Una vez que el archivo sea desarrollado la clase Echo, alerta al administrador de tráficos de red que la detección se llevó a cabo exitosamente (Sufian Hameed, 2016).

Según el ajuste realizado en Tshark pudieron constatar la detección de los ataques, para lo cual emite lo más relevante de lo que se desarrolló en la fase de detección, incluyendo la información de: marcas de tiempo, IP de fuente, IP de destino, protocolo de paquete y un resumen sobre los encabezados de los paquetes que se listan a continuación son aquellos que se encuentran registrados en los archivos de registro: TCP (SYN), HTTP, UDP, ICMP.

Zentyal es un servidor del tipo "Linux Small Business Server", que permite gestionar todos sus servicios de red a través de una única plataforma. Es una puerta de enlace para sus redes, así como una infraestructura de servidor, UTM (Unified Threat Manager), Oficina y Comunicaciones. Todas estas características están plenamente integradas y son fáciles de configurar, lo que realmente ayuda a ahorrar tiempo a los administradores de sistemas.Un servidor Zentyal puede actuar como puerta de entrada en un escenario muy común. Zentyal proporcionará la infraestructura básica de red, balanceo de carga entre dos proveedores de Internet, cortafuegos y caché HTTP proxy y filtrado de contenido. Zentyal is a Linux Small Business Server, it lets you manage all your network services through one single platform. It’s a Network Gateway.https://www.linux-party.com/35-linux/7048-zentyal-como-puerta-de-enlace-gateway-la-instalacion-perfecta.

Los Next-Generation Firewalls de FortiGate utilizan procesadores de seguridad especialmente diseñados y servicios de seguridad de información de amenazas de FortiGuard Labs para dar la mejor protección y alto rendimiento, incluyendo el tráfico cifrado. FortiGate reduce la complejidad con la visibilidad automatizada de las aplicaciones, los usuarios y la red, además proporciona clasificaciones de seguridad para adoptar las mejores prácticas de seguridad.

Los firewalls de última generación de SonicWall le dan la seguridad, control y visibilidad de red que las organizaciones necesitan para innovar y crecer rápidamente. Nuestros galardonados hardware y firewalls virtuales se integran fuertemente con una amplia gama de productos, servicios y tecnologías para crear una solución de alto rendimiento que se personaliza para cumplir con sus necesidades. https://www.sonicwall.com/es-mx/products/firewalls/.

Dentro de las funciones que tienen los Firewall Sonic Wall están:

- Bloquea más ataques con las tecnologías Real-Time Deep Memory Inspection (RTDMI) y Reassembly-Free Deep Packet Inspection (RFDPI).
- Evita amenazas avanzadas con la prevención de amenazas en la caja y en la nube que incluye sandbox de múltiples motores, anti-malware, prevención de intrusión, filtrado web y más.
- Descifra e inspecciona el tráfico TLS/SSL y SSH en tiempo real.
- Obtiene un rendimiento más rápido a través de la arquitectura de un hardware de múltiples núcleos a alta velocidad.
- Añada una red inalámbrica de alta velocidad utilizando el controlador inalámbrico integrado.

A medida que los arquitectos de seguridad consideran cómo proporcionar una protección integral contra amenazas para las organizaciones, al incluir la prevención de intrusiones, el Web Filtering, el antimalware y el Application Control, se enfrentan a un gran obstáculo de complejidad al administrar estos productos puntuales sin integración y sin visibilidad.

La gestión unificada de las amenazas simplifica la seguridad UTM es necesario por que proporciona el paquete de seguridad de red definitivo con todo lo que necesita en un solo dispositivo modular. Simplifica la seguridad TI sin la complejidad de múltiples soluciones independientes. La interfaz intuitiva ayuda a crear políticas rápidamente para controlar los riesgos para la seguridad, mientras que los informes claros y detallados le ofrecerán toda la información que necesita para mejorar la protección y el rendimiento de la red.

5.12 Descripción de características de Sophos UTM

Sophos UTM es una solución basada en el sistema operativo Suse EnterpriseLinux 11 y sus principales componentes están basados en proyectos Open Source, tales como:
- IPS basado en Snort

- DNS basado en Bind.
- VPN SSL basado en OpenVPN
- Firewall basado en Netfilter.
- Firewall de aplicaciones web basado en ModSecurity.
- IPSec basado en StrongSwam.
- Módulo de encriptación basado en GNU PG.
- Datos de configuración, logs y reporteria son guardados en una base de datos de PostgreSQL.

5.12.1 Los requerimientos de hardware para la instalación de Sophos UTM

- Disco Duro: Mínimo 20 Gb en discos IDE, SCSI o S-ATA.
- Procesador: Dual Core de al menos 2.0 Ghz.
- Memoria RAM: Mínimo 1024 MB
- Mínimo 2 tarjetas de red.

5.12.2 Módulos que contiene SOPHOS UTM

Los módulos que contienen Sophos UTM y los cuales serán habilitados en la Institución son los siguientes

5.12.2.1 Módulo Management

Este módulo permite realizar configuraciones iníciales y básicas del sistema tales como; fecha y hora, ubicación de zona horaria, aplicación de licencia, actualizaciones del sistema, configuración de la interfaz de configuración web, respaldo y restauración de configuraciones, administración de notificaciones, portal de usuario, administración centralizada de UTM, alta disponibilidad, entre otras.

Gráfico n° 2: Opciones del módulo management

5.12.2.2 Módulo Definitions & Users

Dentro de este módulo se puede realizar la creación de objetos a ser usados en las diferentes configuraciones dentro de todos los módulos del UTM, los objetos que se pueden definir son; objetos de red, objetos de servicios (puertos), objetos de periodo de tiempo, usuarios y grupos. Así también se puede realizar integración con servidores de autenticación y habilitar la autenticación de doble factor la cual se integra con la herramienta Google Authenticator.

Grafico n° 3: opciones del módulo Definitions & user

5.12.2.3 Módulo Interfaces & Routing

En este módulo se puede configurar las interfaces de red, calidad de servicio, soporte para el protocolo IPv4 y IPV6, opciones de enrutamiento; estático, OSPF, BGP, PIM-SM.

Grafico n° 4: Operaciones de modulo interfaces & routing.

5.12.2.4 Módulo Network Services

Se encuentran los principales servicios de red que debe haber en toda infraestructura, DNS para la resolución de nombres, DHCP para la asignación dinámica de direcciones IP y NTP para la sincronización del tiempo en los distintos dispositivos.

Gráfico n° 5: opciones del módulo network services

5.12.2.5 Bind

Como se mencionó anteriormente el servicio de DNS que usa Sophos UTM es basado en BIND. El servicio DNS es el encargado de traducir las direcciones IP que se encuentran en formato numérico, a nombres de dominio que se encuentran en formato alfanumérico, los cuales son nombres fáciles de recordar para el ser humano al momento de referirse a determinado servidor local o sitio web alojado en Internet. Por ejemplo, al servidor con la dirección privada IP 10.10.10.7 está asociado el nombre de dominio srv00prd01.abc.local, o al sitio web en internet www.fanaticosdelared.com está asociada la dirección IP pública 23.67.189.74.(Paul Albitz y Cricket Liu, 2006)

5.12.2.6 Módulo Network Protection

Es uno de los módulos más importantes y funcionales en Sophos UTM para controlar la seguridad en la red, ya que éste contiene funciones como; firewall, protección contra amenazas avanzadas, sistema de prevención de intrusos IPS, entre otros.

Gráfico n° 6: opciones del módulo network protection

5.12.2.7 Netfilter

El firewall de Sophos UTM es basado en el proyecto Netfilter. Netfilter o también llamado iptables es una herramienta desarrollada para funcionar como cortafuegos o firewall la cual permite realizar filtrado de paquetes y también traducción de direcciones de red o NAT (Network Address Translation por sus siglas en ingles). Con Netfilter se pueden crear reglas de firewall que procesen a los paquetes aceptándolos, descartándolos o rechazándolos.

5.12.2.8 Snort

Snort es un potente proyecto Open Source, el cual es implementado por Sophos UTM para su sistema de prevención de intrusos. Alejandro Gramajo de Baicom Networks, define a Snort en su artículo “Introducción a conceptos de IDS y técnicas avanzadas con Snort” de la siguiente manera:

Snort es rápido, flexible y un NIDS Open Source. Empezó a fines de 1998 como un sniffer. Con licencia GPL version 2. Por default utiliza técnicas de detección de firmas y anomalías no estadística.

Puede correr en varios modos de ejecución

- Sniffer.
- Packet Logger.
- NIDS.
- IPS con FlexResp o Inline. Requiere libnet. Para Inline se necesita libipq.

El “engine” del Snort está dividido en componentes:

- Decodificador del paquete (PacketDecoder)
- Toma los datos de libpcap olibipq.
- Preprocesadores (Preprocessors o InputPlugins)
- Motor de detección (DetectionEngine)
- Comparación contrafirmas

- Logging y sistema de alerta (Logging and AlertingSystem)
- Plugins de salida (Output Plugins).

5.12.2.9 Módulo Web Protection

El modulo Web Protection se encarga del filtrado de navegación y permite establecer políticas de acceso a Internet mediante perfiles de navegación tanto por usuario como por direcciones IP. Los perfiles de navegación pueden configurarse de manera permisiva o restrictiva, permitiendo variedad de opciones como selección de categorías de sitios web predefinidas, ingreso de sitios web personalizados, revisión antivirus en el filtrado de navegación.

Gráfico n° 7: opciones del módulo web protection

5.12.2.10 Módulo Email Protection

El modulo email protection brinda protección de trafico SMTP y POP3, es decir, los protocolos encargados del envío y recepción de correos electrónicos, evitando el *SPAM* (correo no deseado) y los correos maliciosos que puedan descargarse. Malware e infectar los equipos de los usuarios. También se puede cifrar o encriptar los correos electrónicos para evitar la fuga de información sensible.

La implementación de este módulo es aplicable a la infraestructura de la Institución ya que la misma cuenta con un servidor de correo de correo local de Microsoft Outlook.

Gráfico n° 8: opciones del módulo email protection

5.12.2.11 Módulo Wireless Protection

Este módulo gestiona la seguridad de redes inalámbricas de la institución y trabaja con diferentes fabricantes de dispositivos Access Point.

5.12.2.12 Módulo Web Server Protection

Web Server Protection es el módulo que contiene el firewall de aplicaciones web, también llamado WAF, el cual protege a los servidores web ubicados dentro de la infraestructura y están publicados a Internet contra las más comunes y avanzadas amenazas que realizan los atacantes a los sitios web, entre las cuales se encuentran los ataques del tipo SQL Injection y XSS.

Gráfico n° 9: opciones del módulo webserver protection

5.12.2.13 Module Site-to-Site VPN

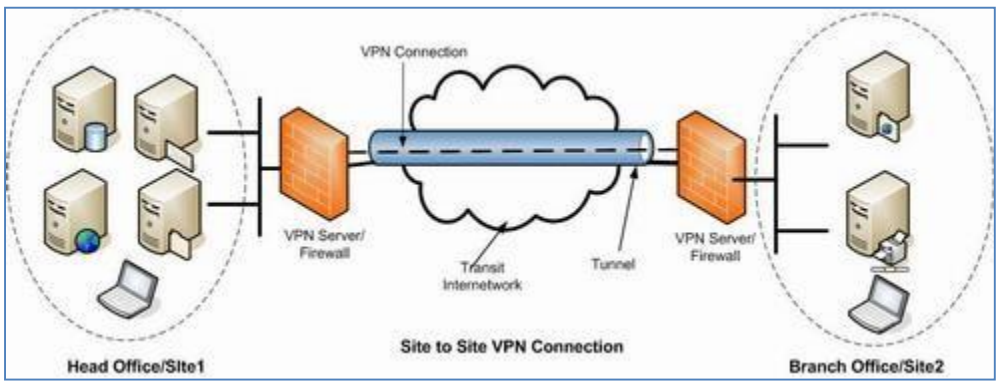
Con la característica de VPN Site-to-Site se pueden realizar configuraciones de túneles virtuales entre dos o más organizaciones para establecer una relación de confianza y garantizar el intercambio de información sobre Internet de manera segura ya que los datos transmitidos por dicho canal pasan cifrados desde el origen hacia el destino.

Gráfico n° 10

Los tipos de VPN Site-to-Site que pueden configurarse en Sophos UTM son:

- Amazon PVC.
- IPsec
- SSL
- Site- to-Site

Gráfico n° 11: ejemplo de diagrama de conexión vpn site-to-site



Fuente: Internet http://rtfq.net/security/firewall-pages/quick-and-dirty-vpn/site-to-site-vpn-problem/.

5.12.2.14 Módulo Remote Access

Este módulo engloba los diferentes tipos de conexiones VPN (Virtual Private Network) cliente, para la conexión remota hacia los servidores y equipos de la carrera de forma segura hacia Internet desde cualquier ubicación. Los tipos de VPN cliente que soporta Sophos UTM son**:**

- SSL
- PPTP (conexión insegura)
- L2TP sobre IPsec
- IPsec
- VPNHTMLv5
- VPN Cisco

Gráfico n° 12: Opciones del módulo remote access

VI. DISEÑO METODOLÓGICO DE LA INVESTIGACIÓN

Partiendo de que el objetivo de la investigación es llegar al conocimiento de la realidad que se estudia, a través de la metodología la cual se basa en un conjunto de métodos y técnicas que forman la teoría y la práctica del conocimiento; el desarrollo del presente proyecto se enmarca en el método cualitativo, el método deductivo y la utilización de técnicas (lectura y observación de campo.).

Esta investigación es de carácter exploratorio - cualitativo utilizándose en ella fuentes primarias y secundarias como base documental para descubrir o afinar la información en el proceso de interpretación, permitiendo analizar a detalle el comportamiento de los tipos de ataque de denegación de servicios, para detectarlo, mitigarlo y ayudar a cuantificar el impacto en las redes internas de los ataques DDoS.

Se realizó una intensa búsqueda bibliográfica, su clasificación y el análisis de la información. Se buscó con ello identificar eventuales ataques DDos que haya sufrido la institución en sus aplicaciones a nivel de capa 7 de aplicación y redes de la DGI y determinar el nivel de conocimientos acerca de los riesgos existentes.

El Método Deductivo, se aplicó en el proyecto al momento de realizar el estudio de la red actual de la DGI y sus puntos críticos hasta llegar al objetivo específico de poder realizar la propuesta de implementación de un UTM firewall de última generación, cuya puesta en producción ayudara en su totalidad protegiendo así los servidores y estaciones de trabajo mediante políticas y buenas prácticas de seguridad para beneficio para la institución.

VII. ANÁLISIS DE MECANISMOS DE DETECCIÓN DE ATAQUES DDOS

Para el análisis de detección de ataques DDoS se utilizó (WAF BIG-IP F5 Networks) es una abreviación en Inglés que significa Firewall para Aplicaciones Web. El WAF BIG-IP F5 Networks es un cerrojo inteligente para la institución. El WAF BIG-IP F5 Networks mantiene el tráfico malicioso fuera del sitio web y de los servidores de nombres. En otras palabras, un WAF BIG-IP F5 Networks es una de la capa de protección que se ubica dentro del diagrama donde están todos los sitios web y el tráfico que recibe a los servidores.

El WAF BIG-IP F5 Networks es un mecanismo que está instalado sobre la red o sobre un servidor web, cuya funcionalidad consiste en analizar, filtrar y bloquear o permitir el tráfico y las peticiones HTTP y HTTPS entrantes a un servidor en función de unas reglas que fueron configurado previamente por con el proveedor. La diferencia principal entre un firewall convencional y un WAF es que el firewall convencional únicamente analiza el tráfico en función de los puertos y las direcciones IP (nivel 3 y nivel 4 únicamente), mientras que un WAF BIG-IP F5 Networks analiza las peticiones y respuestas recibidas y enviadas por el servidor, es decir, analiza el tráfico hasta nivel capa 7 o de aplicación.

Los firewalls de redes y locales por sí solos no pueden evitar que los hackers entren a tu sitio web y servidores. Muchas de estas soluciones no son efectivas cuando se trata de detener el tráfico malicioso en línea.

Hay tres mecanismos clave dentro de WAF BIG-IP F5 Networks que ofrecen para la funcionalidad y protección de la red como son: El Procesamiento (PVA), un proxy completo arquitectura y un validador de protocolos. Gestión de memoria y una personalizada configuración complementa, este trío de mecanismos de detección para ayudar a la Institución a repeler ataques.

7.1 Procesamiento de PVA

El PVA es un procesador de hardware personalizado de WAF BIG-IP de F5 Networks y especialmente diseñado que ayuda a escalar en un orden de magnitud por encima de las soluciones solo de software. La tecnología PVA es totalmente consciente de la sesión y contiene código de mitigación para ataques de red comunes como inundaciones SYN.

7.2 Arquitectura de proxy completo

Las soluciones creadas sobre una arquitectura de proxy completo pueden ser agentes de seguridad activos porque su arquitectura los hace parte del flujo de tráfico, no simplemente dispositivos muestreando ese tráfico. Los productos que son proxies completos brindan una seguridad inherentemente mejor porque terminan activamente el flujo de datos, esencialmente creando un "espacio de aire" modelo de seguridad dentro del producto. Con proxies completos de WAF F5, se puede examinar el tráfico proveniente del cliente antes de enviarlo al nivel de aplicación, asegurando que el tráfico malicioso nunca pasa la barrera del poder. El tráfico que regresa del servidor puede ser completamente examinado antes de que se considere aceptable devolverlo al cliente, por lo tanto, asegurarse de que los datos confidenciales, como los números de tarjeta de crédito o de Seguridad Social nunca cruzó la barrera del poder.

7.3 Validación de protocolo

Un tercer método de ataque a la red consiste en enviar datos con formato incorrecto, como paquetes con combinaciones inválidas de banderas o fragmentos incompletos. Estos ataques pueden ser muy efectivos porque atan la CPU o la memoria de los dispositivos que los examinan. A menudo, el número de ciclos de CPU dedicados a defender el paquete enana el procesamiento que se necesita para iniciar el paquete, lo que hace que este método se conozca como ataque asimétrico. Tales datos inválidos y ataques asimétricos son mitigados por la validación del protocolo tecnología de productos WAF BIG-IP de F5 Networks. En la validación del protocolo, comprende el protocolo de red esperado del tráfico destinado a cada aplicación y puede descartar tráfico mal formado antes de que penetre más profundamente en el centro de datos.

Sophos XG 210 tiene el mecanismo de mitigación para proteger su red de un ataque DDoS, mediante el uso de políticas de prevención de intrusiones en el módulo de políticas IPS se agrega la nueva política DDoS protection.

VIII. PLAN DE MITIGACIÓN DE ATAQUES DDOS

El presente plan de mitigación tiene como alcance, definir las actividades de contingencia a ejecutar, en caso de incidentes relacionados con la seguridad de la infraestructura y servidores, causados principalmente por ataques a los sitios y servicios en línea de la Institución. Mitigar los ataques que se presenten a los sitios y servicios en línea de la Institución, mediante el monitoreo de la infraestructura y servidores, así como bloqueo del origen de los ataques.

Contar un plan de mitigación de DDoS marcará la diferencia entre horas o días de caos en toda la Institución y una respuesta rápida y ordenada que mantenga la normalidad del negocio. Aplicar la propuesta de un plan de mitigación de DDoS para nuestra Institución, anticiparemos los puntos únicos de fallo. Los atacantes DDoS aprovecharán cualquier posible punto de fallo, como sitios web, aplicaciones web, interfaces de programación de aplicaciones (API), sistema de nombres de dominio (DNS) y servidores de origen, así como centros de datos e infraestructuras de red y comprobar la capacidad de mitigación de DDoS de nuestro proveedor de servicios de Internet (ISP).

Si un ataque DDoS contra nuestro sitio web pone en riesgo a otros clientes del ISP, este seguramente bloquee (desvíe) todo el tráfico, y su sitio web quede inoperativo de forma indefinida. Esto conllevara a preguntar al ISP:

- El tamaño del ataque DDoS que intentará mitigar antes de bloquear todo el tráfico del sitio. Además, qué requisitos tendrá para restaurar el servicio de Internet.
- La capacidad disponible que tiene en la red, además de los picos de tráfico normales.
- Monitoree ataques volumétricos. Siempre en necesario mantener una página web abierta para indicarle cuando el ataque pueda haber acabado (o haber sido mitigado).

8.1 Pasos del plan de Mitigación de Ataques DDoS

1- Se realizará en todo momento monitoreo y seguimiento a los estados de los servicios, mediante las herramientas como el ASA, IPS y WAF BIG-IP de F5 Networks trabajando en conjunto las áreas de comunicación y bases de datos.

2- En caso de detección de ataques, se procederá a analizar las fuentes del mismo, determinar el tipo de ataque, servicios afectados y proceder a mitigarlo mediante la aplicación de bloqueos en las diferentes capas que puedan estar afectadas, Bloqueos IP mediante el IPS, Bloqueo de la direcciones IP atacantes por medio del ASA Cisco y los módulos que bloqueo que contiene el WAF BIG-IP de F5 Networks.

3- En caso de ataques volumétricos de DDoS que saturen alguno de los enlaces de datos existentes, se procederá a realizar traslado de conexiones de VPN de las entidades externas hacia el otro centro de datos Alterno que existe, en coordinación con las entidades que usan dicho VPN (Bancos, Registro público, Policía Nacional, Consejo Supremo, Alcaldía Municipal de Managua, etc.) hasta que sea mitigado el ataque con el UTM de Sophos.

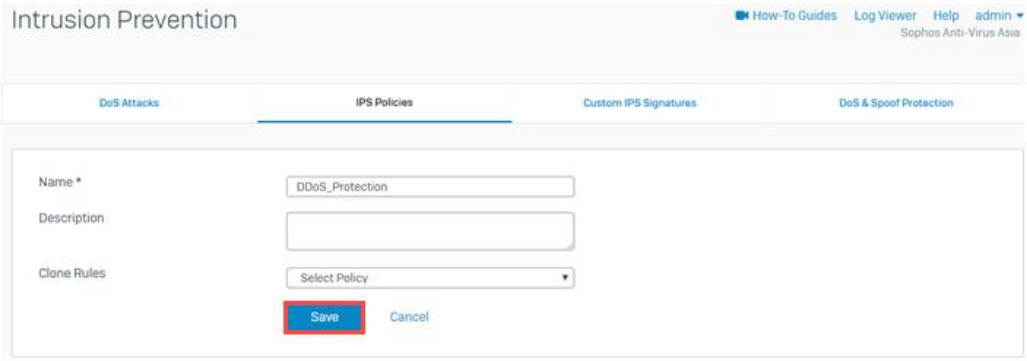
4- Es importante señalar que de presentarse algún tipo de ataque volumétrico DDoS de saturación cuyo origen sea fuera de Nicaragua, la única opción disponible de mitigación sería el bloqueo mediante Sophos UTM y el bloqueo de acceso externo por parte del **ISP**, de modo que solo el peering local podría tener acceso a los servicios, pero habría afectación del servicio de correo electrónico externo y navegación por internet. Así mismo, usuarios que acceden fuera de Nicaragua, no podrían acceder a los servicios.

5- Para desencadenar el proceso de mitigación, es necesario tener elementos que indiquen la ejecución de un ataque, para lo cual es necesario realizar monitoreo de forma permanente, que se estará realizando por las diferentes áreas de la Oficina de apoyo tecnológico. Para realizar el monitoreo, se utilizarán las siguientes herramientas:

- **Herramienta de monitoreo Nagios, para ver el estado, CPU, conexiones, Memoria y uso de disco.**
- **Monitoreo de conexiones desde en el IPS.**
- **Monitoreo en el WAF BIG-IP de F5 Networks**
- **Chequeo de ancho de banda por las herramientas proporcionadas de los ISP.**

6- La mitigación de los ataques DDoS se realiza por medio de la política creada en el módulo prevención de instrucciones, políticas IPS.

1. Vaya a **Prevención de intrusiones> Políticas IPS.**
2. Haga clic en **Agregar** para crear una nueva política de prevención de intrusiones denominada **DDoS_Protection** .



3. Haz clic en **Guardar** .
4. Clickea en el icono de la política **DDoS_Protection** .
5. Haga clic en **Agregar** para crear una nueva regla llamado **DDoS_Signatures** .
6. En el campo **Filtro inteligente** , escriba "ddos" (sin las comillas) y luego presione Intro.
7. Establezca la **acción** para **soltar el paquete** .

Fuente: https://community.sophos.com/kb/en-us/123182

7- Actividades a realizar en caso de ataques. Esto fue elaborado por nosotros mismo.

Evento	Acción a realizar	Tiempo estimado de la acción	Responsables
Ataques a sitios web de tipo inyección, crossite, etc.	Este tipo de ataques son bloqueados por el WAF, se realizará monitoreo y seguimiento de las IP para realizar bloqueo a nivel de ASA e IPS. Se determinarán	5 minutos por acción, tomando en cuenta el tiempo de detección y reporte a los encargados de realizar bloqueo	Unidad de comunicaciones Unidad de bases de datos

Evento	Acción a realizar	Tiempo estimado de la acción	Responsables
	analizarán IP y se bloquearán		
Ataques a servidor de correo electrónico.	Son bloqueados automáticamente después que una IP realiza 3 intentos a una cuenta de correo, se realizará monitoreo para bloqueo a nivel de IP por medio de script en el servidor	5 minutos por acción, tomando en cuenta el tiempo de detección y reporte a los encargados de realizar bloqueo	Unidad de comunicaciones Unidad de bases de datos
Ataques de DDoS a Centro de datos Managua	Se analizará tráfico y se realizará traslado de operaciones y conexiones de las entidades externas al otro centro de datos. Se notificará a los encargados de redes de las entidades afectadas: instituciones Bancarias, Alcaldía Municipal, Registro Público, Policía Nacional, Consejo	1 hora aproximadamente. El cual podría cambiar debido a que se debe coordinar con los encargados de las otras entidades.	Unidad de comunicaciones Personal de las entidades externas.

Evento	Acción a realizar	Tiempo estimado de la acción	Responsables
	Supremo Electoral, Ineter		
Ataques de DDoS a Centro de datos León.	Se analizará tráfico y se corta el acceso de internet del centro de datos alterno.	15 minutos.	Unidad de comunicaciones
Ataques simultáneos DDoS a los dos centros de datos	Coordinar con los ISP para bloquear tráfico externo de Nicaragua y solo permitir tráfico de peering local	1 hora aproximadamente	ISP Unidad de comunicaciones

IX. IMPLEMENTACIÓN DEL GESTOR UNIFICADO DE AMENAZAS (UTM)

El uso de soluciones UTM para proteger las redes solía ser una medida parcial, aunque se conseguían ahorros de recursos y facilidades de uso, había que renunciar a ciertas capacidades de protección. Hoy en día, proteger las redes con soluciones UTM es toda ventaja. Además de disfrutar de los estándares de seguridad más altos, es posible integrar multitud de funciones de protección en una sola plataforma y añadir otras cuando sean necesarias.

En cuanto a las amenazas de tipo externo, la tendencia actual es evitar la utilización de equipos dispersos para cada una de las amenazas y en su lugar, concentrar todos los recursos y herramientas en un solo equipo, denominado sistema **UTM** (Unified Threat Management) o sistema de tratamiento unificado de amenazas. Estos equipos incluyen funcionalidades como las siguientes:

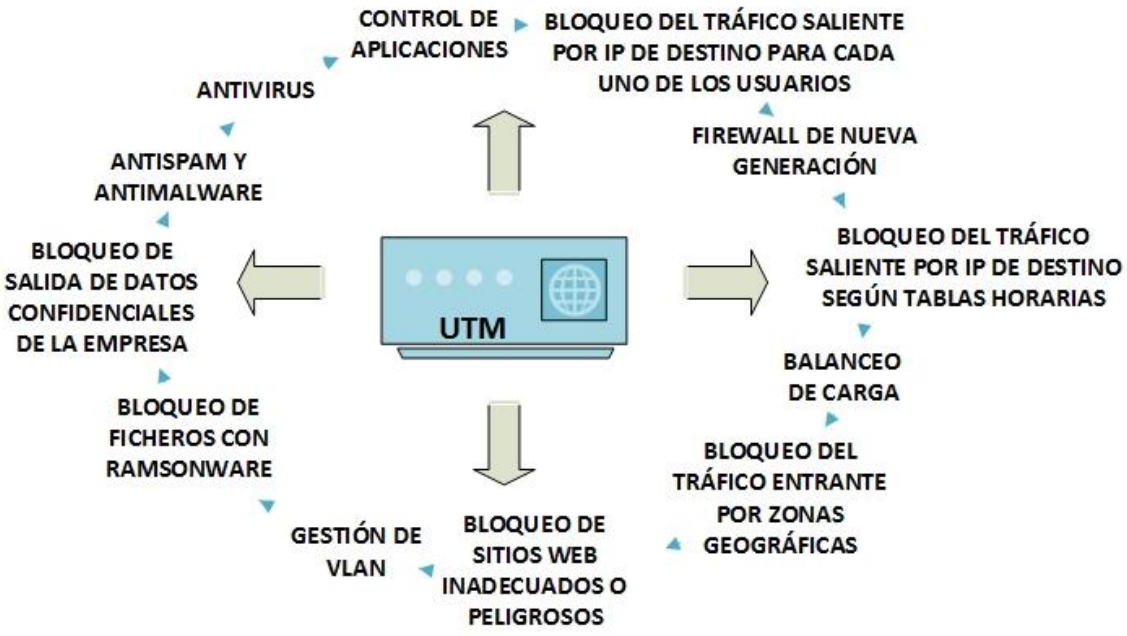


Grafico n° 13 Funciones de los equipos de tratamiento unificado de amenazas (UTM)

La implementación del Firewall UTM incluye un análisis y levantamiento de la red actual, una reingeniería de la estructura de la red LAN y de servidores de la DGI, posterior a un análisis detallado de la situación inicial de la misma y así poder aplicar las mejoras a este diseño. Se instalará y configurará el dispositivo por Hardware UTM, luego del análisis y comparación de los diferentes UTM que cumplan con los requerimientos y dimensionamiento de tráfico de la DGI, teniendo en cuenta Los líderes del mercado según el cuadrante de Gartner; como: Fortinet, Check Point Software Technologies y Sophos.

El alcance de esta propuesta de solución es para la red institucional de la DGI, cubriendo la protección de las diferentes subredes administrativas y sucursales, roles de servidores, conexiones físicas y lógicas, reglas de Firewall, direccionamiento IP, canales VPN, permisos de navegación, escaneo de antivirus, cifrado, filtrado de navegación, escaneo antispyware, control a nivel de aplicaciones, control de tráfico de red, Firewall de aplicaciones web, etc.

9.1 Identificación de la infraestructura actual de la red institucional de la Dirección General de Ingresos (DGI)

La red LAN y WAN actual de la Dirección General de Ingresos (DGI), actualmente está configurada e interconectada con diferentes dispositivos de seguridad con elementos activos y pasivos de conectividad a internet y la red Intranet; la interconexión entre la WAN y las redes LAN a través de servidores de correo, proxy y Web, Switch Cisco de capa 3, Swicth de acceso, equipos de seguridad ASA, WAF BG IP Networks, IPS McAfee, DLP y una consola de antivirus que administra todos los usuarios de la Institución.

La conectividad y red corporativa herramienta de monitoreo Nagios de codigo abierto, que vigila los equipos para ver el estado o carga del CPU, conexiones,

memoria y uso de los disco y estado de los puertos.Cuenta con una herramienta de monitoreo de red con licenciamiento IPS McAffee que gestiona sobre una plataforma unificada el monitoreo de servidores, servicios y equipos de comunicación de toda la red, mejorando el tiempo de respuestas en casos de problemas fortuitos mediante un sistema de alarma (por correo) para prevenciones tempranas frente a problemas de hardware o software en los diferentes entornos de la infraestructura tecnologica.

Monitoreo por medio de WAF BIG IP F5 Network, defensa proactiva contra ataques, que monitorea y bloquea cualquier trafico malicioso HTTP/S que viaje a la aplicación web, proteccion frente a denegacion de servicios de capa 7, que protege las aplicaciones web de la organización, bloqueando la variedad de ataques que apuntan a comprometer los sistemas.

La conexión WAN se hace por medio de Fibra optica proveida por el ISP Alliance (Proveedor de Servicios de Internet). La conexión hacia las aplicaciones o servicios como correo electronico, pagina web, protegidos por un WAF BIG IP F5 Network de aplicaciones en modo software y monitoreados.

Los servicios de transmision de datos hacia las diferentes entidades como MHCP, bancos, administracion de rentas y agencias fiscales interconectados al Firewall ASA principal y protegidos o monitoreados por un IPS McAfee.

La red de cableado interna es estructurada con cable UTP, categoria 5. Cuenta con un area de Data Center y Rack de datos principal.

La red LAN esta dividida en varias VLAN: VLAN de produccion donde estan todos servidores en produccion; Vlan Manager, estan los usuarios que tienen acceso a todas las vlan; Vlan Desarrollo, todos los programadores y analistas y la Vlan

Internet que esta como una DMZ(zona desmilitarizada) donde estan todos los equipos que estan de cara al contribuyente.

La infraestructura de usuarios finales es Windows 10 con arquitectura de 32 y 64 bits. La conexión hacia los puntos de red corporativa se realiza a traves de switches de capa 2 en su mayoria cisco; distribuidos en diferentes gabinetes Rack e interconectados por el backbone o enlaces principales por medio de fibra optica multimodo.

La siguiente figura muestra el esquema detallado de conectividad de la red actual de la Dirección General de Ingresos (DGI).

DIAGRAMA GENERAL DE LA RED LAN-WAN DE LA DGI

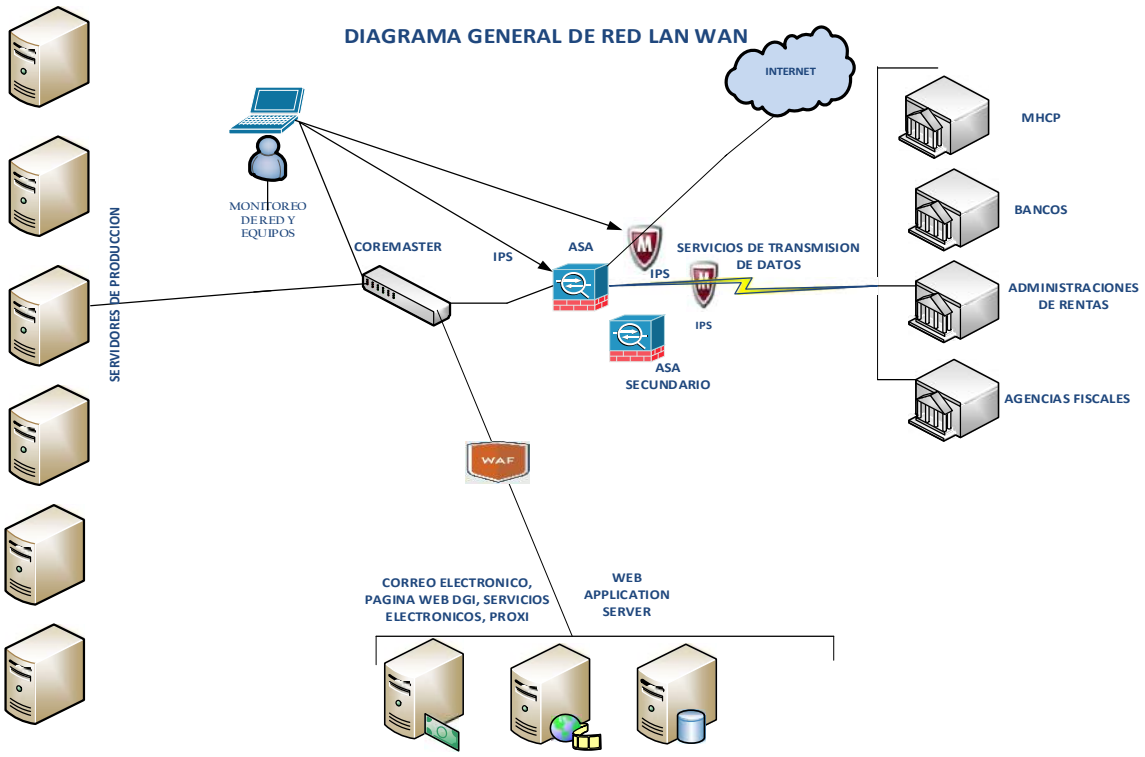


Grafico n° 14 Fuente : DGI

Para hacer una implementacion adecuada y eficiente del Firewall de última generación UTM, se propone el siguiente esquema de Red para la DGI, con el fin de facilitar la gestión centralizada de amenazas y monitoreo eficiente de la Red.

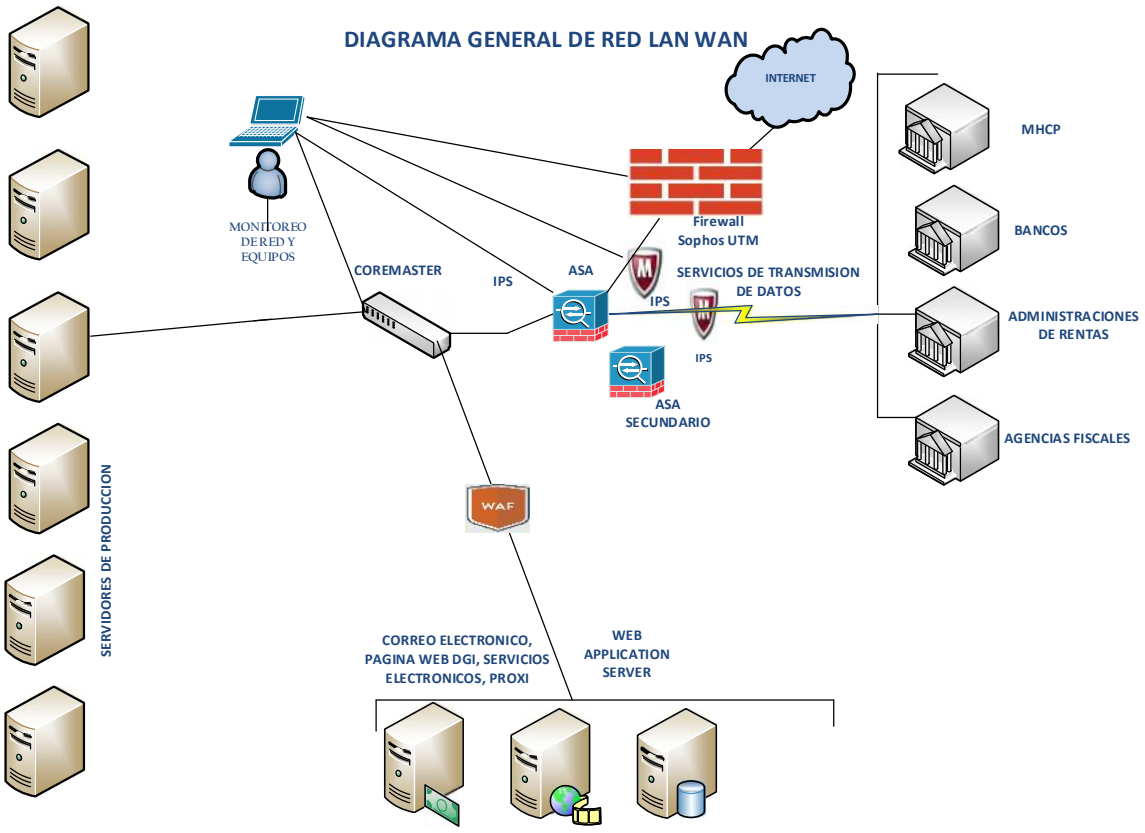


Grafico n° 15

Esta arquitectura facilitará el cumplimiento de las politicas de seguridad, el rendimiento de la red y simplicidad de la misma.

Como filtro de la red se plantea el Firewall UTM a implementar y configuracion de las siguientes funcionalidades:

- Monitoreo en tiempo real de tráfico de red.
- Balanceo y alta disponibilidad de enlaces de internet.
- Enrutamiento: Estático, OSPF, BGP Multicasting.
- Agregado de enlaces.
- Sistema de detección y prevención de intrusos (IPS).

- Posibilidad de alta disponibilidad en hardware.
- Servicios de red: DNS, DHCP, NTP.
- Soporte de IPv6.
- NAT: Destination NAT, Source NAT, Full NAT.
- Filtrado de navegación web.
- Protección antivirus y antispyware perimetral.
- Control de aplicaciones.
- Protección anti spam, antiphising y antivirus de correo.
- Cifrado de correo electrónico.
- VPN site-to-site: IPSec y SSL.
- Acceso remoto vía VPN SSL, IPSec, PPTP, L2TP/IPsec.
- Web Application Firewall (Firewall de aplicaciones web).
- Protección contra amenazas avanzadas.

El firewall bastión garantizará en un alto porcentaje que los ataques que se sufran de manera externa serán contenidos y repelidos; pero lo más importante alertará a los administradores de estos ataques, para tomar acciones correctivas.

Se implementarán reglas de filtrado de paquetes diseñadas, de acuerdo a la nueva topologia y politicas de seguridad. Se mantendrá un control total sobre los protocolos y puertos que se estén ejecuntando sobre la red corporativa de la DGI.

9.2 Análisis de diferentes tecnologías firewall UTM

Tomando como referencia el análisis de tecnologías Firewall del 2018 presentado en el cuadrante de Gartner (Empresa consultora y de investigación de tecnologías de la información con sede en Stanford Connecticut, Estados Unidos), se observa cuales son las tecnologías que están como lideres del sector en lo referente a firewall de próxima generación.

Según Gartner el mercado de los Firewall sigue evolucionando en productos de nueva generación, con nuevas características para mejorar el cumplimiento de las políticas(aplicaciones y usuarios), detectar nuevas amenazas mediante los sistemas de prevención de intrucciones (IPS), el uso de las VPN (redes privadas virtuales), manejo de servicios web o transferencias de datos seguros o cifrados mediante la utilización del protocolo Secure Sockets Layer (SSL).

En la figura siguiente observamos los firewall de gestión unificados de amenazas UTM empresariales que se encuentran en el Cuadrante Mágico de Gartner.

Cuandrante Mágico de Gartner para firewall UTM de última generación

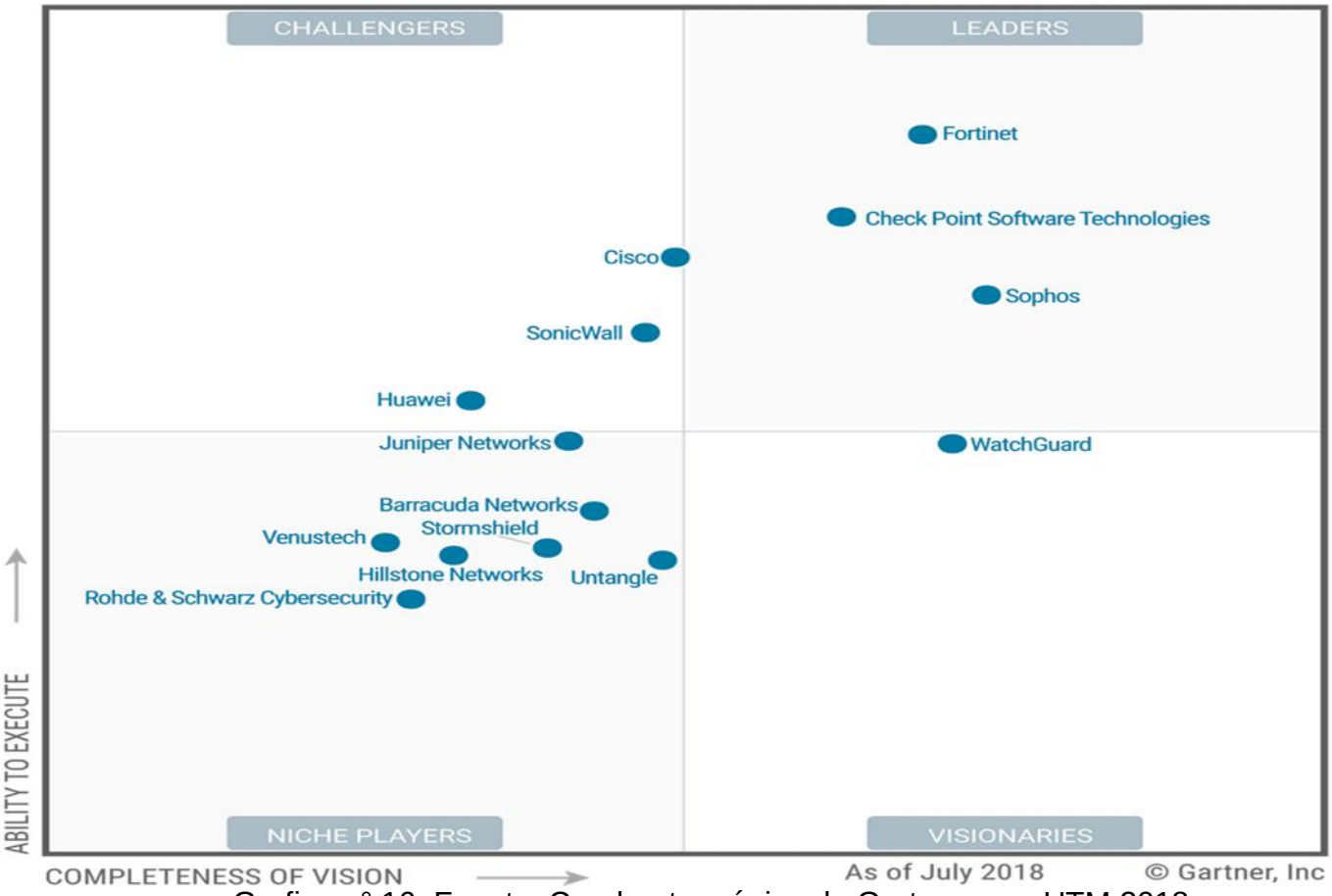


Grafico n° 16: Fuente: Cuadrante mágico de Gartner para UTM 2018

A continuación, se realiza la comparación de las características de seguridad y funcionalidades independientes de los dispositivos UTM de las principales marcas líderes en el mercado.

9.3 Análisis de firewall Fortinet UTM

La tecnología de Firewall de Fortinet o Fortigate UTM, es uno de los líderes del mercado de soluciones de seguridad unificados según el cuadrante de Gartner, proporciona una amplia protección contra amenazas, es una Appliance de alto rendimiento que simplifica la infraestructura de seguridad para la empresa reduciendo el riesgo de las amenazas cibernéticas.

Fortinet desarrollo el Firewall **FortiGate 300D** con el objetivo de satisfacer las necesidades de las medianas y grandes empresas que requieren una seguridad de red de alto rendimiento a precios competitivos, por lo tanto, **FortiGate 300D** proporciona un rendimiento superior a los firewalls de su categoría, ofreciendo el mejor precio de la industria por gigabit protegido.

La serie FortiGate-300D ofrece protección real e integral, conteniendo todos los beneficios de una UTM (Gestión Unificada de Amenazas) Fortinet. Proporciona aceleración de firewall en todos los tamaños de paquetes, aceleración de procesamiento de contenido UTM, acceso remoto seguro y VPN de alta velocidad para un rendimiento y protección superior.
FortiGate-300D se instala fácilmente, descargando automáticamente actualizaciones regulares para ofrecer protección contra los virus más recientes, las vulnerabilidades de redes y ataques de gusanos, spam y phishing y sitios web maliciosos sin necesidad de la intervención de ningún administrador.

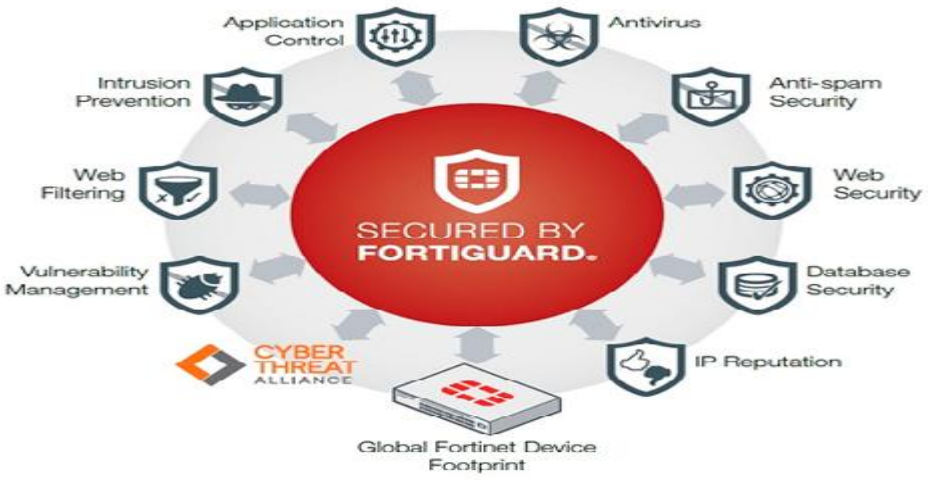
Sus funcionalidades corren sobre su sistema operativo FortiOS 6.2 (última versión), que introduce nuevas mejoras e innovaciones.
Las principales funcionalidades incorporadas a destacar:

- Habilita el Security Fabric de Fortinet para obtener mayor protección de los dispositivos del Internet de las cosas (IoT) a la nube, lo que ayuda a los clientes a reducir y administrar la superficie de ataques.Soporte de nuevos elementos (FortiMail,FortiWeb,FortiADC,FortiDDOS, FortiWLC)SD-WAN (mejoras en IPSEC, incluyendo agregación de túneles y Per Packet Load Balacing, mejoras en la monitorización de SLAs y Dashboards históricos) para acceder de forma segura a las aplicaciones en la nube.

Fortinet ha conseguido que la Gestión Unificada de Amenazas supere las fronteras y dé el salto hacia la denominada XTM (**eXtensible Threat Management**) que es la nueva generación de sistemas UTM.

Este producto es muy fácil de implementar, y además, su desempeño destaca por el alto rendimiento de UTM, firewall, VPN, IPS, aplication control, web filtering, antivirus, antispam, DLP y otros.

Grafico n° 17. En el siguiente gráfico se muestran las características incorporados en el UTM Fortinet



Fuente: https://www.z-net.com.ar/blog-post/ventajas-de-fortinet-por-sobre-otras-marcas/

Los servicios de suscripción FortiGuard, que se encargan de mantener todos los sistemas de FortiGate debidamente actualizados, en tiempo real y de forma automática, incluyendo las funcionalidades de los firewalls de nueva generación, es decir filtrado de puertos, filtrado de aplicaciones, y accesos de aplicaciones por perfiles o grupos de usuarios, además de la protección contra virus, malware, spam, entre otros.

La funcionalidad FortiASIC; permite ejecutar las funciones de seguridad acelerando el procesamiento, ofreciendo de esta forma un desempeño óptimo en el manejo de ancho de banda.

Respaldado por los servicios FortiCare para soporte técnico. Fortinet ofrece también una plataforma en la nube, para la gestión de políticas de seguridad y configuración centralizada, con una capacidad de gestión de 10.000 Dispositivos Fortinet.

Esta funcionalidad se conoce como FortiManager, FortiAnalyzer y FortiCloud. La gama de soluciones de Fortinet es: protección de amenazas avanzadas basadas en Sandbox o cajas de arena, protección de aplicaciones web, protección de correo electrónico, protección de DDoS, controlador de descubrimiento de aplicaciones, gestión de identidad de usuarios y control de tráfico LAN y WAN.

Características

- 8 Gbps rendimiento de Firewall (1518/512/64 byte UDP packets)
- 7 Gbps rendimiento Ipsec VPN (512 byte packets)
- 6.000.000 sesiones concurrentes
- 200.000 nuevas sesiones/segundo
- 10.000 políticas de Firewall
- 2.000 Gateway-to-Gateway IPsec túneles VPN

9.3.1 Administración simple

La administración basada en la nube permite que su personal sea más eficiente al habilitar una fuerza laboral móvil.

9.3.2 Amplié rápido y fácilmente

El Fortinet Security Fabric le permite agregar productos sin problemas a medida que su organización crece, como endpoints, sandboxing y más. Sandboxinges altamente eficaz y se integra en toda la superficie de ataque con el intercambio dinámico de información para detectar malware avanzado en todos los vectores de ataque.

FortiClient fortalece la seguridad de los endpoints a través de la visibilidad, control y la defensa proactiva integrada.

9.3.3 Libere recursos

La administración unificada y las redes que se amplían a medida que usted crece le permiten liberar personal con recursos limitados para que se centre en otras actividades.

9.4 Análisis de Firewall UTM SOPHOS de última generación

Sophos UTM proporciona el paquete de seguridad de red definitivo con todo lo que necesita en un solo dispositivo modular. Simplifica la seguridad TI sin la complejidad de múltiples soluciones independientes. La interfaz intuitiva ayuda a crear políticas rápidamente para controlar los riesgos para la seguridad, mientras que los informes claros y detallados le ofrecerán toda la información que necesita para mejorar la protección y el rendimiento de la red.

El modelo XG Firewall ofrece la mejor protección contra las últimas amenazas avanzadas como el ransomware, la criptominería, bots, gusanos, hackers, filtraciones y amenazas avanzadas recurrentes.

- Potente tecnología de espacio seguro de Sandstorm.
- Deep Learning con inteligencia artificial.
- IPS de máximo rendimiento.
- Protección avanzada contra amenazas y redes de bots.
- Protección web con AV dual, emulación de JavaScript e inspección SS.

Integra parte de la mejor tecnología líder de última generación Intercept X para endpoints, como la prevención de exploits y la protección CryptoGuard para identificar exploits de malware y ransomware antes de que puedan acceder a su red. En combinación con el sistema de prevención de intrusiones (IPS) de máximo rendimiento.

Todas las funciones están disponibles en todos los dispositivos Firewall, VPN, ATP, IPS, email, filtrado web y control de aplicaciones, dispositivos de hardware, virtuales, software o en la nube, interfaz web intuitiva, informes incorporados en todos los modelos, autenticación de doble factor y contraseñas de un solo uso en muchas áreas y Controlador inalámbrico integrado.

Ofrece un licenciamiento flexible, se pueden adquirir las licencias de los módulos de forma individual o elegir uno de los paquetes preconfigurados de licencia lo que mejor se ajusta a las necesidades de la empresa.

La tecnología de Sophos UTM se puede implementar en la plataforma que se requiera: hardware, software, virtual o incluso en la nube.

Su sistema operativo basado en Linux incluye un firewall de red básico gratuito que proporciona funciones de seguridad fundamentales como firewall,

herramientas de red, enrutamiento y acceso remoto seguro. Además, su sistema por módulos permite añadir capas de protección a medida que evolucionan las necesidades.

9.4.1 Network Protection

Bloquea los ataques sofisticados que los firewalls no pueden detener por sí solos.

- La protección avanzada contra amenazas (ATP) combina varias tecnologías para identificar y bloquear el tráfico saliente dirigido a servidores de comando y control. Al combinarla con la protección web, se consiguen espacios seguros selectivos basados en la nube que mejoran continuamente la protección.
- Sistema de protección contra intrusiones configurable y protección contra ataques de denegación de servicio.
- Los túneles SSL e IPsec ofrecen conexiones flexibles VPN de acceso remoto y de sitio a sitio

9.4.2 Email Protection

Bloquea el correo no deseado y los virus, y protege los datos confidenciales.

- Proporciona cifrado sencillo del correo electrónico sin infraestructuras y prevención de fugas de datos basada en políticas para proteger los datos sensibles y cumplir las normativas fácilmente.
- Permita que los usuarios gestionen su propia cuarentena de correo no deseado y realicen búsquedas en los registros de correo personalizados.
- Impida la entrada de mensajes de correo electrónico infectados en los buzones y proteja los mensajes confidenciales contra accesos ilegales.

9.4.3 Wireless Protection

Ofrece conexiones Wi-Fi seguras en cuestión de minutos.

- Configure fácilmente puntos de acceso inalámbricos con autenticación de backend, cupones o SMS

- Funciona mejor junto con Sophos Mobile Control (SMC) para proporcionar control de acceso a la red para dispositivos móviles.

9.4.4 Web Protection

Permite proteger a los empleados contra las amenazas web y controlar el uso que hacen de Internet.

- Cree políticas de filtrado URL e imponga cuotas de navegación y navegación web por tiempo de forma sencilla para usuarios individuales y grupos
- Restrinja el uso de aplicaciones no deseadas y otorgue prioridad a los recursos vitales para la empresa
- Pruebe las políticas para comprobar si funcionan y cree informes dinámicos

9.4.5 Web Server Protection

Refuerza las aplicaciones y los servidores web para garantizar el cumplimiento de las normativas con un firewall de aplicaciones web.

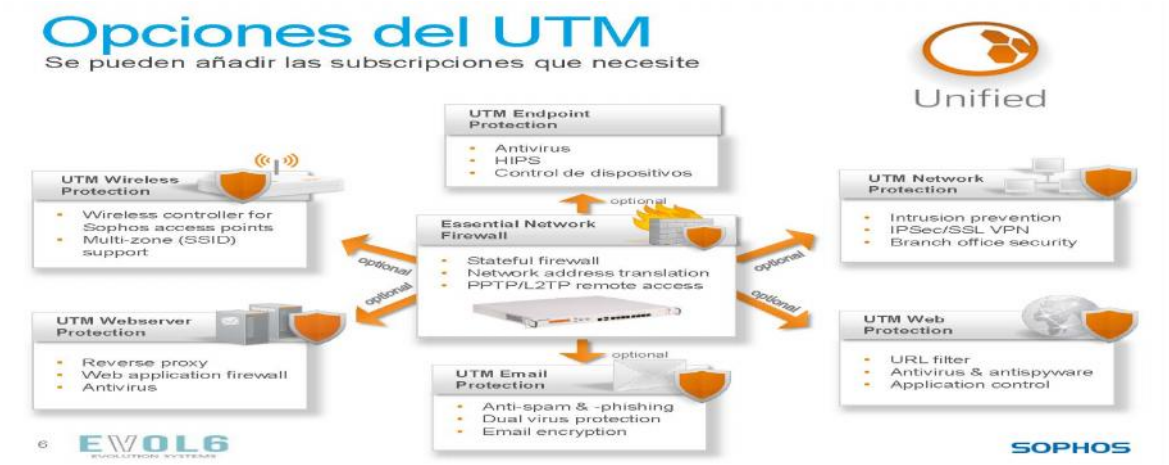
- La autenticación de servidores proxy inversos proporciona un nivel adicional de seguridad para las aplicaciones empresariales
- Evite ataques mediante inyección de SQL, secuencias de comandos entre sitios, cruce de directorios salto de directorio, manipulación de cookies y mucho más.

9.4.6 Sandbox Protection

Proporciona una protección de espacio seguro avanzada basada en la nube.

- Protección contra ataques dirigidos, visibilidad y análisis
- Bloquea amenazas evasivas con informes granulares por incidentes
- Basado en la nube significa sin despliegue ni impacto en el rendimiento

Grafico n° 18. En el siguiente Grafico muestra las funciones del UTM SOPHOS



Fuente: https://docplayer.es/537447-Seguridad-completa-en-una-caja-sophos

9.4.7 Sophos Red

Reenvía todo el tráfico al dispositivo Sophos UTM central para proteger las sucursales. No es necesaria formación técnica para instalarlo ni mantenimiento continuo.

9.4.8 Puntos de acceso Wi-Fi

Puntos de acceso sin necesidad de configuración protegidos al instante por el dispositivo UTM, lo que permite crear redes de malla seguras.

9.4.9 Clientes VPN

Las VPN SSL o IPsec seguras o nuestras VPN HTML5 sin cliente proporcionan a los trabajadores móviles e internos acceso remoto seguro desde cualquier lugar y en cualquier momento.

9.4.10 UTM Manager gratuito

Administra de forma centralizada varios dispositivos UTM a través de túneles de VPN IPsec; implementa políticas con solo unos cuantos clics. El dispositivo de presentación de informes Sophos iView amplía y mejora la presentación de

informes integrada con informes de cumplimiento, informes consolidados a través de múltiples UTM y gestión de registros a largo plazo.

9.5 Mejoras en su conectividad

Le permiten adaptar la conectividad de su dispositivo 1U o 2U a los cambios en su entorno Los módulos 3G/4G añaden conectividad a cualquier unidad SG 125(w) o 135(w) usando nuestro módulo complementario.

9.5.1 Segundo módulo Wi-Fi

Para añadir una segunda radio a su unidad SG 135w para una mejor cobertura y rendimiento. Transceptores requeridos para todas las interfaces SFP, SFP+ y QSFP+ modulares

9.6 Fuente de alimentación redundante

Para añadir una segunda fuente de alimentación a cualquier dispositivo 1U o 2U SG 1xx de escritorio.

9.7 UTM que proporciona portal VPN

Basado únicamente en el navegador
Sin Java o Active-X
Sin cliente software

9.8 Expone riesgos ocultos

Ofrece una visibilidad sin procedentes sobre los usuarios de mayores riesgos, apps desconocidas, amenazas avanzadas y mucho más.

9.9 Bloquea amenazas desconocidas

La tecnología avanzada que ofrece protege su red contra ransomware y amenazas avanzadas, como ISP de primera categoría, espacio seguro en la

nube, antivirus dual, control web y de aplicaciones, protección del correo electrónico y un firewall de aplicaciones web integral. Es fácil de configurar y administrar.

9.9.1 Responde automáticamente a incidentes

Es la única solución de seguridad para redes que puede identificar totalmente el origen de una infección en la red y responder limitando el acceso a los otros recursos de red de forma automática. Esto gracia a la tecnología única de Sophos Security Heartbeat que comparte el estado y datos de telemetría entre los endpoints de Sophos y su firewall.

9.10 Análisis de Firewall Check Point UTM

Check Point líder en el Cuadrante Mágico Gartner 2018 en UTM, es el séptimo año consecutivo que la empresa de ciberseguridad Check Point figura como líder Unified Threat Management.

Check Point Software Technologies Ltd. es un proveedor líder de soluciones de ciberseguridad para gobiernos y empresas a nivel mundial. Sus soluciones protegen a sus clientes de los ciberataques con una tasa de captura de malware, ransomware y otros tipos de ataque líder en el mercado. Ofrece una arquitectura de seguridad multinivel que protege la información de las empresas almacenada en la nube, en la red y en los dispositivos móviles, además del sistema de gestión de la seguridad más completo e intuitivo. Check Point protege más de 100.000 organizaciones de todos los tamaños.

Sus soluciones ayudan a las empresas a proteger sus datos contra amenazas y ataques avanzados de quinta generación. El firewall de próxima generación de Check Point identifica y controla las aplicaciones por usuario y escanea el contenido para detener las amenazas.

9.10.1 Características de Check Point UTM

Protección contra amenazas
Anti-malware
Sandboxing basado en red
Sandboxing basado en la nube
Sandboxing archivo
firewall
Sistema Anti-bot
Seguridad web
Control de aplicaciones
GeoIP bloqueado
SSL proxy de avance
Descifrado SSL
Seguridad de correo electrónico
Filtro spam
Prevención de malware
Filtrado de contenidos
Protección de spam saliente
Cortafuegos de red
IPV6
Conformación de tráfico y colas de prioridad
Inspección de estado

Inspección profunda de paquetes
Capacidades adicionales
IPS
WAF
VPN
Opciones de implementación
Nube, hardware, dispositivo virtual

El CheckPoint es un UTM sólido con muchas características excelentes. Este dispositivo incluye protección contra un firewall y un sistema IPS conocido como SmartDefense, así como antivirus de puerta de enlace, antispyware y filtrado de contenido web, puerto DMZ, soporte NAT, filtrado URL, soporte VLAN, soporte VPN. Esta herramienta también proporciona bloqueo de aplicaciones IM y P2P y mantiene los protocolos comerciales, como FTP y VoIP, a salvo de ataques.

Este producto se administra a través de aplicaciones de administración de Check Point y hay varias de ellas. Hay uno para la administración y varios otros para informes, monitoreo y otras funciones. Estas aplicaciones deben instalarse para administrar el dispositivo y no son muy intuitivas de usar.

Las opciones de soporte de Check Point van desde el plan de soporte estándar que brinda asistencia telefónica durante el horario comercial normal con el envío al día siguiente de dispositivos de reemplazo, hasta el plan de soporte premium que brinda asistencia las 24 horas del día, los 7 días de la semana con envío de reemplazo el mismo día, hasta el premium + 4H plan que proporciona un ingeniero calificado en el sitio dentro de las cuatro horas para resolver cualquier problema relacionado con el dispositivo. También hay un área de soporte gratuito en el sitio web que incluye documentación, descargas y un foro de usuarios.

Con un precio que comienza en alrededor de $ 3,500, este producto es un valor bastante promedio para el dinero. Es rico en funciones, pero también es difícil de usar y requiere acostumbrarse.

Fortalezas: un IPS solido con muchas políticas predefinidas activadas de forma predeterminada

Debilidad: difícil de usar y administrar

Ver tabla de comparación en el (anexo 13.3) de las características de seguridad independientes de los dispositivos UTM de las principales marcas

9.11 Solución propuesta de implementación de un gestor unificado y amenazas de acuerdo a un análisis de las tecnologías.

Una vez realizado el análisis comparativo y tomando en cuenta las ventajas que ofrecen los sistemas de Gestión Unificadas de Amenazas y considerando que su principal características es la integración de diferentes módulos de seguridad que garantizan la adecuada protección de la red sin degradar su rendimiento ya que cuentan con hardware y software optimizado para realizar una completa gestión de amenazas al tiempo que reducen los costos de gestión en vista de que no será necesario administrar varias soluciones parciales de diferentes proveedores, se propone a la institución la implementación de la tecnología **UTM SOPHOS XG 210** de próxima generación en su modo hardware, ya que es la que más características técnicas favorables y funcionalidades de seguridad que se ajustan a los requerimientos de la infraestructura de red de la DGI. También porque es fácil de configurar y administrar gracias al panel de control configurable en tiempo real, la flexibilidad de las licencias modulares, y las intuitivas definiciones de objetos de red reutilizables.

Por lo tanto, se requiere adquirir el activo de hardware Firewall UTM-SOPHO XG 210 de nueva generación para su implementación e instalación en la infraestructura de red de la DGI.

9.11.1 Aspectos a considerar

- Implementación de dispositivo firewall UTM en la topología de la institución
- Servicios de administración, gestión y operación de la plataforma de seguridad
- Capacitación de personal en sitio para la gestión de la plataforma de seguridad
- Administración centralizada de los perfiles y configuraciones de las soluciones que compongan el sistema de seguridad
- Configuración acceso externo a las aplicaciones de la institución de forma segura

Hay dos factores principales que definieron el haber seleccionado la solución Firewall UTM **SOPHOS XG 210** para la implementación como son el costo de licenciamiento y la operatividad; en cuanto a costos de licenciamiento encontramos que por ejemplo Sophos es uno de los proveedores que comercializa su producto a precios accesibles, pero también tiene licenciamiento free.

Sophos UTM es una solución sin igual en cuanto a flexibilidad de despliegue: hardware, software, virtual y en la nube con opciones sencillas para una alta disponibilidad, agrupaciones en clúster, conectividad de oficinas remotas, conexión inalámbrica y administración e informes centralizados. Y a diferencia de la competencia, no tiene que hacer concesiones en lo que respecta a las funciones y al rendimiento al elegir. Todas las funciones están disponibles en todos los modelos y formatos.

Su velocidad de rendimiento es excepcional potente y rápido, utilizando tecnología multinúcleo de Intel, unidades de estado sólido, y escaneo de contenido en memoria acelerado. Su interfaz de usuario (IU) simple e intuitiva que facilita las tareas de gestión.

La solución propuesta consiste principalmente, en la implantación de un Firewall UTM todo en uno funciones de seguridad integradas en una sola plataforma; el cual sería el encargado de controlar los paquetes de entrada y de salida de la empresa, estableciendo las reglas de filtrado de la red, para que toda la empresa tanto en su red de visitantes, como en su red empresarial, estén protegidos, y así brindar la seguridad informática que requiere la institución.

La implementación de un Firewall perimetral de nueva generación UTM que integra varias funciones de protección en un solo punto en la red, garantizará una mejor gestión de seguridad informática de manera centralizada; esto mitigará las vulnerabilidades de seguridad presentes actualmente.

El UTM incluye funcionalidades de Firewall, filtrado de navegación Web, protección antivirus, administración de ancho de banda, sistemas de prevención de intrusos, entre otras funcionalidades que ayudarán a fortalecer la seguridad del tráfico de red entrante y saliente, garantizando la confidencialidad, integridad y disponibilidad de la información.

9.12 Costos de implementación Sophos XG 210

El presupuesto destinado por la DGI para la adquisición del Gestor Unificado de Amenazas es de $ 8,500.00 (Ocho mil quinientos dólares americanos) con impuestos incluidos.

OFERTA ECONOMICA

Firewall Sophos XG 210			
Item	Descripcion	Cant.	Precio
1	Equipo Appliance Firewall XG 210 Rev.3 TotalProtect, Licenciamiento Total Protect por 12 meses	1	$7,300.00
2	Licencia Base de Firewall	1	
3	Licencia Network Protection	1	
4	Licencia Web Protection	1	
5	Licencia Sandstorm	1	
6	Implementacion	1	$0.00
7	Soporte tecnico SISAP 7x24, por 12 meses	1	$0.00
		SUB TOTAL:	$7,300.00
		IVA	$1,095.00
		TOTAL	$8,395.00

- Moneda: Dólares de los Estados Unidos de Norteamérica.
- Tiempo de entrega 30 días hábiles

Oferta Proporcionada por el proveedor SISAP.

Tabla Presupuesto Referencial UTM

TECNOLOGÍA	VALOR EN DÓLARES U$
UTM FORTIGATE- 300D	10,612.00
UTM SOPHO XGC210	8,395.00

Con esta tabla presupuestaria referencial que tiene costo beneficio para la DGI según presupuesto asignado para la adquisición del UTM unificado por el precio, funcionalidad y cumple con todo lo requerido es Sophos.XG 210 que es un firewall de última generación**.**

9.12.1 Características técnicas de los servicios de seguridad requeridos.

La solución deberá tener las siguientes características de rendimiento de acuerdo al estimado de conexiones concurrentes:

- Mínimo 1000000 conexiones concurrentes
- Funcionalidad de UTM incluido
- Mínimo 2 puertos 10/100/1000 Ethernet y 2 puertos GbE SFP
- Contar con fuente redundante de potencia
- IPS Throughput (HTTP)>= 6 Gbps
- IPSec Throughput >= 17 Gbps
- SSL-VPN Throughput >= 500 Gbps
- Firewall 16 GBPS
- NGFW 2,9 GBPS
- VPN 1,45 GBPS
- Sistema de prevención de intrusiones 3 GBPS
- AV (proxy) 2,3 GBPS
- Interfaces Ethernet
- 6x GbE cobre, 2x GbE SFP
- Ranuras FleXi Port 1
- Módulos FleXi Port (opcional)*
- GE cobre de 8 puertos
- GE SFP de 8 puertos
- SFP 10 GE de 2 puertos
- SFP 10 GE de 4 puertos
- QSFP 40 GE de 2 puertos
- GE cobre de 4 puertos
- con omisión LAN
- PoE GE de 4 puertos

9.12.2 Funcionalidades de Seguridad a implementar o activar en el UTM de Sophos XG 210.

Como base en la instalación e implementación propuesta del firewall UTM de nueva generación incluirá las siguientes funcionalidades de gestión unificada de amenazas:

Funcionalidades a Implementar
Autenticación
Network Protection
Creación de Reglas de Firewall
IPS
ATP
Web Protection
URL Filtering
Sandstorm
IPS
Application Control
Configuraciones Avanzadas
15 AP Sophos modelos (55 100)
OTP para ingreso a webadmin
VPN Usuario (SSL)
LACP con equipo L3 HP

9.12.3 Cómo proteger la red contra ataques DoS y DDoS utilizando Sophos XG Firewall

Sophos XG Firewall previene ataques DoS y DDoS mediante la funcionalidad del IPS.

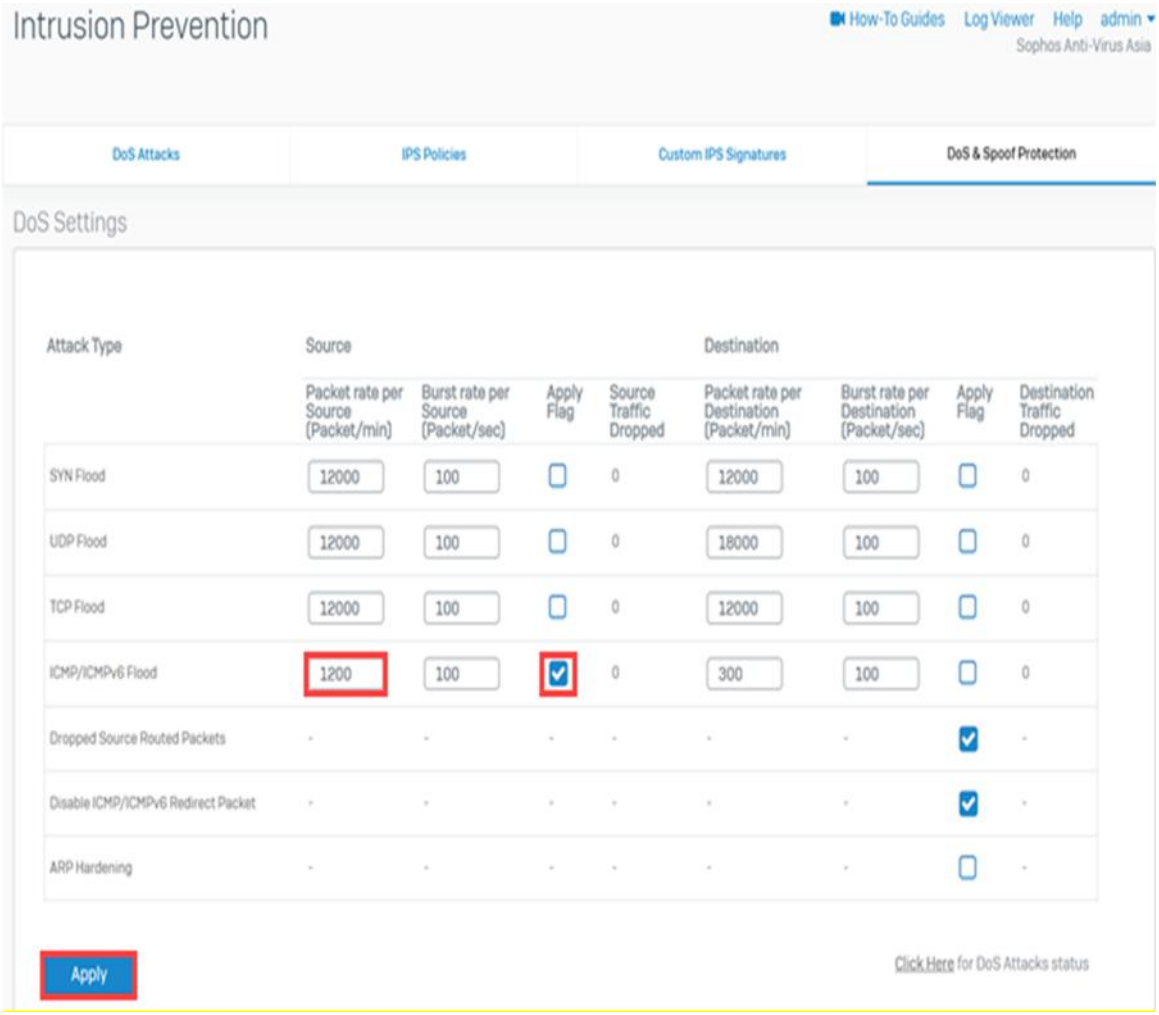
9.12.4 Protegiendo su red de un ataque DoS

Se puede proteger la red contra ataques DoS para el tráfico IPv4 e IPv6 configurando la Configuración DoS adecuada en el Firewall Sophos XG. Puede configurar los ajustes de DoS siguiendo los pasos a continuación:

Prevención de intrusiones> DoS y protección contra falsificaciones.

Establecer las tasas de paquetes y ráfagas en la sección Configuración de DoS de acuerdo con el tráfico de su red y marque el indicador Aplicar junto al parámetro para permitir la exploración del tipo de tráfico respectivo.

En la figura siguiente podemos observar un ejemplo, hemos establecido la tasa de paquetes por fuente (paquete / min) como 1200 para ICMP / ICMPv6 Flood y verificamos el indicador aplicando junto para permitir el escaneo del tráfico ICMP e ICMPv6.



Le damos cli en aplicar para que la configuración este salvada.

9.12.5 Protegiendo su red de un ataque DDoS

Para proteger la red contra ataques DDoS mediante el uso de políticas de prevención de intrusiones. Tenemos en cuenta que las firmas DDoS solo están disponibles en el modelo XG210.

9.12.6 Pasos para configurar una política en módulo IPS del UTMI.

1. Ir a Prevención de intrusiones> Políticas IPS.
2. Haga clic en Agregar para crear una nueva política de prevención de intrusiones denominada DDoS_Protection.
3. Clic en Guardar.
4. Haga clic en el icono de la política DDoS_Protection.
5. Haga clic en Agregar para crear una nueva regla denominada DDoS_Signatures.
6. En el campo Filtro inteligente, escriba "ddos" (sin las comillas) y luego presione Intro.
7. Establezca la acción para soltar el paquete.
8. Haga clic en Guardar y luego haga clic en Guardar nuevamente para guardar la política.
9. Vaya a Firewall y aplique la política de prevención de intrusiones a la regla de usuario / red.

9.12.7 Información Adicional

La protección DoS funciona por base de origen / destino, por lo que la tasa de paquetes y la tasa de ráfaga se aplicarán por origen / destino.

Sophos XG Firewall buscará primero una regla de omisión y luego aplicará protección DoS para el tráfico restante.

9.12.8 Flujo de muestra

Sophos XG Firewall permite los primeros 100 paquetes en ráfaga y, después de 100 paquetes, comprobará la velocidad de entrada de los paquetes. Si el paquete cae por debajo de la velocidad configurada, entonces aceptará el paquete. Si el paquete supera la velocidad configurada, declarará la fuente como un flooder y luego descartará los paquetes.

Cuando llega un nuevo paquete desde la dirección IP del flooder, verificará si el último paquete de la misma fuente llegó en 30 segundos o no.
Si el último paquete estuvo dentro de los 30 segundos, entonces caerá y registrará el paquete como una inundación.

Si el último paquete no estuvo dentro de los 30 segundos, entonces Sophos XG Firewall incluirá en la lista blanca la fuente y permitirá el tráfico. Si en el caso de que Sophos XG Firewall no recibiera ningún tráfico del flooder después de 30 segundos, no se incluirá en la lista blanca y seguirá estando bajo las direcciones IP del flooder.

9.13 Ventajas y desventajas de un UTM

Ventajas	Desventajas
Se tiene un único dispositivo para la simplicidad de la arquitectura de red.	Las aplicaciones individuales pueden no tener todas las características de los dispositivos independientes
Funciones integradas de seguridad para una administración más simple	Implementación de dispositivos redundantes son requeridos para evitar puntos únicos de falla
Reportes unificados para dar una imagen completa de la red y su estado de seguridad	Procesadores compartidos pueden requerir grandes actualizaciones para todo el dispositivo, o descargas de aplicaciones por separado, para evitar problemas de rendimiento.

El personal de tecnologías de la información tendrá menos dispositivos sobre los cuales requerirá capacitación	Punto único de compromiso en caso de existir vulnerabilidades en el sistema.
UTM es un término que se refiere a un firewall de red con múltiples funciones añadidas. Trabajando a nivel de aplicación. Realiza el proceso del tráfico a modo de proxy, analizando y dejando pasar el tráfico en función de la política implementada en el dispositivo.	Genera un impacto en la latencia y ancho de banda de la red cuando el sistema no se encuentra bien configurado

9.14 Requerimientos de instalación y configuración

El firewall UTM Sophos XG 210 Total Protect de última generación requiere de los siguientes elementos de instalación: alimentación: 100-240VAC (50-60Hz), espacio en rack: 1U,19” standard rack, conectividad: cableado UTP, temperatura de operación 20 grados Celsius.

La DGI cuenta con cableado estructurado de red, espacio el Rack donde instalar el nuevo equipo, interfaces disponibles 10/100/1000 el switch Core master para conectar el nuevo equipo de seguridad, conectividad eléctrica respaldada por dos UPS de 20 Kva, aires acondicionado de precisión para mantener la temperatura adecuada en el centro de datos y piso falso que debe tener un centro de datos donde están instalados los Rack.

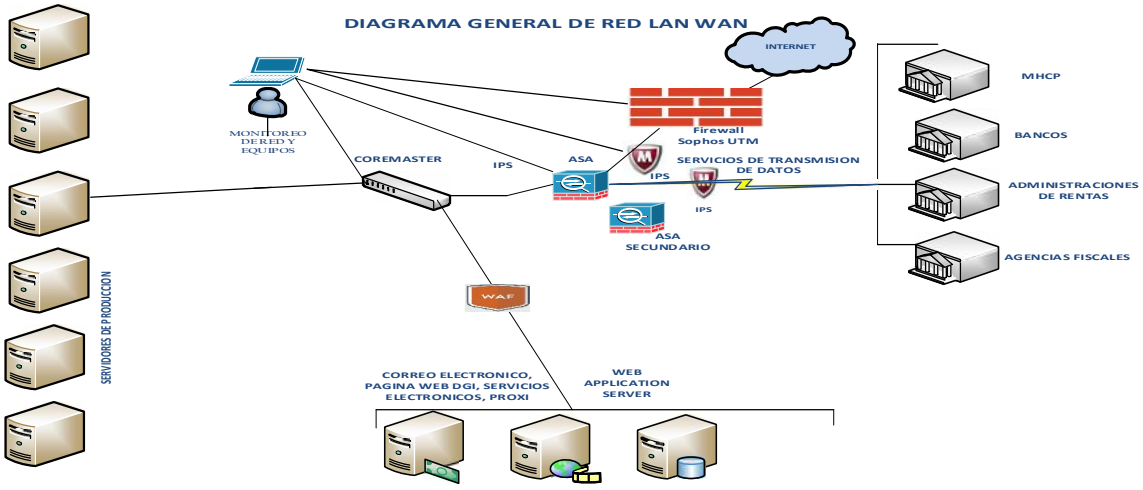
9.15 Diseño y arquitectura de la solución

La solución de seguridad de firewall propuesta a la alta gerencia de la DGI consta de un equipo unificado Sophos SG210 -. El dispositivo quedara configurado como un firewall unificado de protección de amenazas entre la red externa y la red interna de la infraestructura de red la DGI y no necesita otro tipo de configuración siempre mientras esté funcionando la solución.

9.16 Diseño lógico a Implementar

A continuación, en la figura, se presenta el diagrama de red lógico final del firewall que se debe implementar en la infraestructura de red de la DGI desde la perspectiva de firewall:

Grafico n° 19



9.17 Perfiles de seguridad

Por medio de los perfiles de seguridad el Firewall Sophos realizará inspecciones sobre el tráfico en búsqueda de intrusos (IPS), malware, (virus-spyware, sandboxing) y acceso no deseado a sitios web (filtro URL).

9.18 Monitoreo de servidores

La protección para los servidores (web, bases de datos, etc.) en una organización no solo se limita a la creación de reglas de seguridad descritas previamente. Se debe tener un monitoreo constante de los logs de Tráfico y Amenazas con el fin de identificar a tiempo las posibles brechas de seguridad que puedan estar siendo usadas con propósitos criminales.

9.19 Resultado e impacto esperado

La red corporativa de la DGI, presenta un grado de complejidad para la administración y control de seguridad, debido a que está diseñada en infraestructuras separadas de conectividad para la red central, sucursales y dependencias de gobiernos y entidades bancarias adicionalmente no se hace un buen manejo de los ancho de banda contratados porque no hay la infraestructura adecuada de un UTM que realice funciones de seguridad a alto nivel y de balanceo o distribución de tráfico para un mejor rendimiento de la red.

Por lo tanto, luego del análisis tecnológico de tecnologías de seguridad y la viabilidad económica se propone a la alta dirección la implementación de Firewall UTM de nueva generación como mecanismo de seguridad de la red corporativa y de servicios virtualizados de la DGI.

Luego de la implementación del Firewall Sophos XG 210 UTM, se evidenciarán resultados positivos de control y uso eficiente de tráfico de red interno y externo, control y prevención de amenazas, bloqueos de páginas maliciosas y no

permitidas, bloqueos de malware, virus, bots de niveles de amenazas críticos, altos, medios y bajos.

La formulación o modificación de las políticas de seguridad informáticade la Institución. Con directrices consulta, socialización e implementación de procedimientos de prevención y mitigación de los riesgos informáticos.

Los procedimientos de seguridad a partir de las políticas establecidas. No basta con implementar un dispositivo tecnológico de seguridad informática, sino la formulación de procedimientos de seguridad en cumplimiento de las políticas establecidas.

9.20 Impacto esperado

Concientizara la Institución sobre la necesidad de establecer mecanismos de protección y prevención de posibles ataques informático a nuestra red, con el riesgo de pérdida de información, pérdida de la confidencialidad de integridad de la información y riesgo en la continuidad del negocio.

La necesidad urgente de la implementación del Firewall de nueva generación. Con la tecnología Sophos UTMXG210 Total Protection se pueden alcanzar las mayores fortalezas de seguridad, debido que cumple con todas las funcionalidades de seguridad de la información y los elementos para prevención contra ataques informáticos. Mayor control sobre aplicaciones. Los mayores ataques informático actualmente se realiza a través de software, también es donde más se detecta huecos de seguridad.

Mayor eficiencia en el manejo de ancho de banda de la red; puesto que se puede controlar el tráfico a través de matrices de perfiles usuarios, identidad de aplicaciones y filtrado de contenidos, entre otros. Cumplir con los requerimientos de protección de los datos personales y confidencialidad de la información.

Con la implementación de la tecnología de seguridad se proyecta tener mitigado los riesgos de seguridad informática y alcanzar una utilización para la sección durante los próximos 5 años.

X. CONCLUSIONES

- Los resultados después de realizar los análisis de mecanismos para la detección de ataques DDoS y su aplicación en los diferentes escenarios, se determina que el mejor mecanismo es WAF BIG-IP F5 Networks, ya que es un mecanismo (Appliance) que se coloca antes de los servidores, efectivamente este niega el acceso a las conexiones nuevas e ilegítimas y se pueden definir tanto lista blancas o listas negras de direcciones IP.

- Con este plan propuesto de mitigación y las medidas a implementarse con el nuevo equipo como es Sophos XG 210 se logrará mitigar cualquier ataque DDoS proveniente desde cualquier lugar, ya sea volumétrico, de aplicación e inteligente.

- La solución propuesta de seguridad propuesta mediante el uso de dispositivos UTM de la marca Sopho XG210 ayudara a proteger los activos informáticos, además permitirá brindar seguridad a las comunicaciones entre sucursales, servicios online que brinda la DGI hacia los contribuyentes.

- Con esta solución propuesta de un Gestor unificado de amenazas (UTM), combina varias funcionalidades (firewall, VPN, antivirus, IDS, IPS y filtrado de contenidos) en un sólo dispositivo, permite garantizar la seguridad centralizada con control completo sobre todas las redes distribuidas.

- Las soluciones de Sophos UTM XG210 se adaptará de forma flexible a las necesidades actuales y futuras de la Institución. Esto debe permitirá la integración de dispositivos adicionales en una única consola de gestión

XI. RECOMENDACIONES

- Para obtener resultados más precisos donde mejore la calidad del mecanismo de detección de ataques DDoS, se puede seguir con la mejora del modelo desarrollado y estableciendo distintos indicadores que se adapten según al tipo de red que se vaya a analizar ya su vez incluir nuevos métodos de detección de ataques de DDoS.

- Tomar este trabajo de investigación como guía para la institución y a nivel superior, para contar con una alternativa de solución ante ataques de DDoS ya su vez generar planes de contingencia en caso de otro tipo de ataques informáticos.

- Teniendo en cuenta que el Sophos XG 210 UMT será la puerta de entrada y salida de todo el tráfico que se direccione hacia Internet, se debe documentar el direccionamiento, segmentación y enrutamiento de toda la red de la institución.

- Actualizar el firmware del software sophos a la ultimación versión recomendada, cargar las licencias adquiridas y dejarlas operativas.

- Se debe capacitar al personal de infraestructura y seguridad informática en la nueva tecnología de firewall de nueva generación adquirida.

- Se recomienda tener personal dedicado solo a la seguridad informática, debido a los requerimientos de administración y monitoreo constante de la red para minimizar de mejor manera los riesgos.

- El factor económico no debe ser una limitante al momento de invertir en tecnologías que permitan desarrollar e implementar políticas de seguridad, contar con mecanismos de control, administración y monitoreo de los dispositivos que conforman la red (Servidores, estaciones de trabajo, equipos de comunicación, etc.) ya que permitirán que la red sea menos vulnerable a intrusiones y denegación de servicio.

- Es indispensable dar a conocer que el equipo de seguridad de la información incluye a todos los empleados, inculcar buenas prácticas de seguridad al personal de la institución puede lograr que mediante capacitación e implementación de tecnología de seguridad perimetral la red sea más segura.

XII. BIBLIOGRAFIA

Armatte, M. (Enero de 2016). *ResearchGate.* Obtenido de https://www.researchgate.net /publication/277268687_La_Nacion_de_ Modelo_en_las_ciencias_solciales

Biazus, &. B. (Diciembre de 2016). *Repositorio Intitucional. Subvertendo um sistema de deteccao de instrusao.* Obtenido de https://repositorio.ufsc.br/handle/123456789/12652

C. Rosales Garcia, M. A. (Mayo de 2011). *Repositoriodigital. Identificacion de ataques de DDoS en redes de datosa a traves de modelo basado en la red bayesiana. IPN, Repositorio Digital-Mediateca, 1-77. .* Obtenido de http://repositoriodigital.ipn.mx/handle/123456789/12652

Cooke, E. J. (2014). *usenix.org. The Zombie Roundup: Understanding, Detecting, and Disrupting Botnets. Arbor Networks. Obtenido de.* Obtenido de https://www.usenix.org/legacy/event/sruti05/tech/full_papers/cooke/cooke_html/

CRS:. (s.f.).

DK, B. J. (2013). *A Machine Learning Perspective.*Obtenido de http://103.4.94.107:8080/xmlui/bitstream/handle/123456789/17621/Network_Anomaly_detection_A_machine_learning perspective.pdf?sequence=1

Feintein. L, S. D. (Abril de 2013). Obtenido de http://ieeeplore.ieee.org/abstract/document/1194894/?reload=true

Garcia, M. D. (2010).

Gupta, B. M. (2012). *tandfonline.com. .* Obtenido de https://www.tandfonline.com/doi/full/10.1080/21642583.2017.1331768

Hoque. N, D. K.-2. (2015). *Botnet in DDoS Attacks_trend and Challenges.*Obtenido de http://www.cs.uccs.edu/~jkalita/papers/2015/HoqueNazrulEEETutorials&Survers2015.pdf

Hoque.N, D. F. (22 de Febrero de 2016).

J. Mirkovic, &. R.-5. (2014). *eecis.edul.edu.* Obtenido de https://www.eecis.edul.edu/~sunshine/publications/ccr.pdf

J.Arzamendia, &. F. (19 de Noviembre de 2016). *researchgate.net.* Obtenido de https://www.t/publication/310496769

Javier Sanchez Gonzales, B. M. (Junio de 2016). *incibe.es.* Obtenido de https://www.incibe.es/extfrontinteco/img/File/intercocert/EstudiosInformes/cert_inf_seguridad_analisis_trafico_wireshark.pdf

Juliette Dromard, V. B.-L. (24 de Febrero de 2017). *Hal.laas.fr/hal-01476103.* Obtenido de https://Hal.laas.fr/hal-01476103

Lau, F. S. (Agosto de 2012).

Malena, G. A. (2013).

Microsoft. (27 de Agosto de 2018). *https://docs.microsoft.com/es-es/azure/application-gateway/waf-overview.* Obtenido de https://docs.microsoft.com/es-es/azure/application-gateway/waf-overview

Mifsud, E. (30 de Septiembre de 2015). *recursostic.educacion.e.* Obtenido de http://recursostic.educacion.es/observatorio/web/es/component/content/article/1065-listas-de-control-de-acceso-acl?start=3

Molina Lorena, F. A.-A. (Junio de 2015).

Narvaez, D. R. (2010). Obtenido de https://journals.openedition.org/polis/10568?lang=pt#ftn2

Narvaez, D. R. (2010). http://journal.espe.edu.ec/index.php/geeks/article/view/249/226. Obtenido de http://journal.espe.edu.ec/index.php/geeks/article/view/249/226

Obtenido, T. (29 de Abril de 2016). *Telectronika*. Obtenido de https://telectronika.com/Articulos/que-es-gn3/

OWASP TOP 10 Project. (28 de Agosto de 2017). Obtenido de https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

Pereira, D. M. (2018).

Roggero, P. &. (2018). *scielo.org.mx.* Obtenido de http://www.scielo.org.mx/scielo.php?script=sci-arttext&pid=s0185-19182015000300227

Saman Zargar, J. &. (2013). Hadoop Base Defense Solutio to Handle Distributed Denial Of Service (DDoS) Attacks. Scientific Research.

Sanmorino, A. &. (2013). DDoS Attack Detection Method and Mitigation Using. ResearchGate, 5.

Sarabia, J. M. (2014). Distribuciones multivariantes con distribuciones condicionadas t de Student. España.

Saravanan, K. &. (Enero de 2012). *Researchgate.net.* Obtenido de https://researchgate.net/publication/51988470_Distributed_Denial_of_service_DDos_attacks_detection_mechanism

Schabel, L. G. (14 de Abril de 2018). *Github.com.* Obtenido de https://github.com/firehol/firehol/wiki/working-with-SYNPROXY

Sufian Hameed, U. A. (Julio de 2016).

XIII. ANEXOS

13.1 Diagrama de funcionamiento de WAF para las redes internas de la DGI.

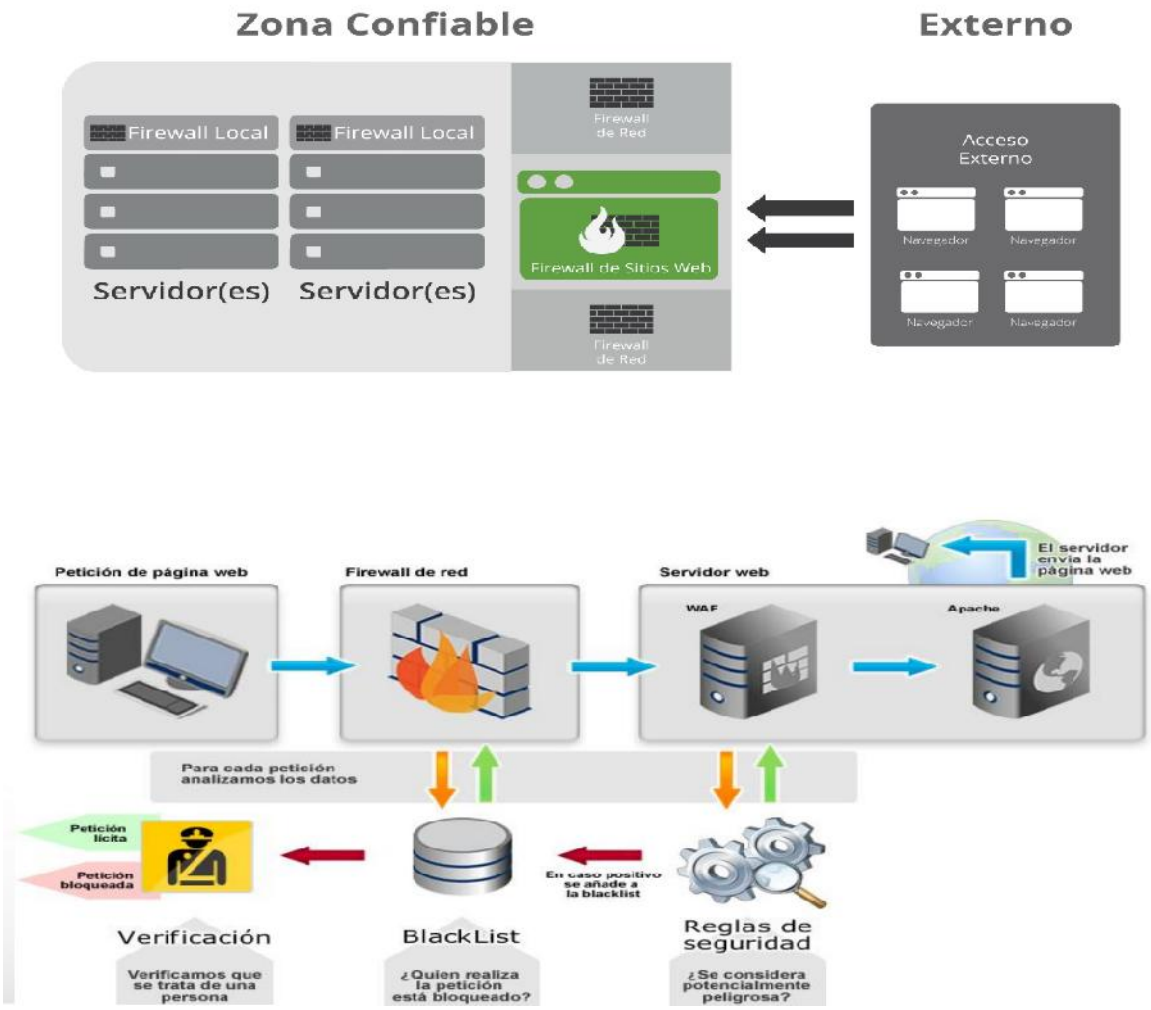


Figura 1.

13.2 Reporte de ataques a la DGI.

	Attack Name	Attack Category	Attack Subcategory	Attack Severity	Attack Count
1	Inbound Link Utilization (Bytes/S...	Volume DoS	over-threshold	Medium	136
2	Outbound Link Utilization (Bytes/...	Volume DoS	over-threshold	Medium	136
3	F2P: BitTorrent File Transfer Han...	Policy Violation	restricted-application	Medium	1
4	HTTP: IIS 6.0 WebDAV Service S...	Exploit	code-execution	High	1
5	RAT: GhostRat Traffic Detected	Malware	botnet	High	1

		Name	Event				Packet Capture	Attacker
			Time	Direction	Result	Attack Count		IP Address
12		Inbound Link Utilization (Bytes/Sec) Too High	Aug 09, 2018 10:48:43	Inbound	n/a	1	Export	---
13		HTTP: IIS 6.0 WebDAV Service ScStoragePathFro...	Aug 09, 2018 10:46:33	Outbound	Attack Blocked	1	Export	39.108.232.0
14		Outbound Link Utilization (Bytes/Sec) Too High	Aug 09, 2018 10:45:27	Outbound	n/a	1	Export	---
15		Inbound Link Utilization (Bytes/Sec) Too High	Aug 09, 2018 10:45:27	Inbound	n/a	1	Export	---

Figura 2.

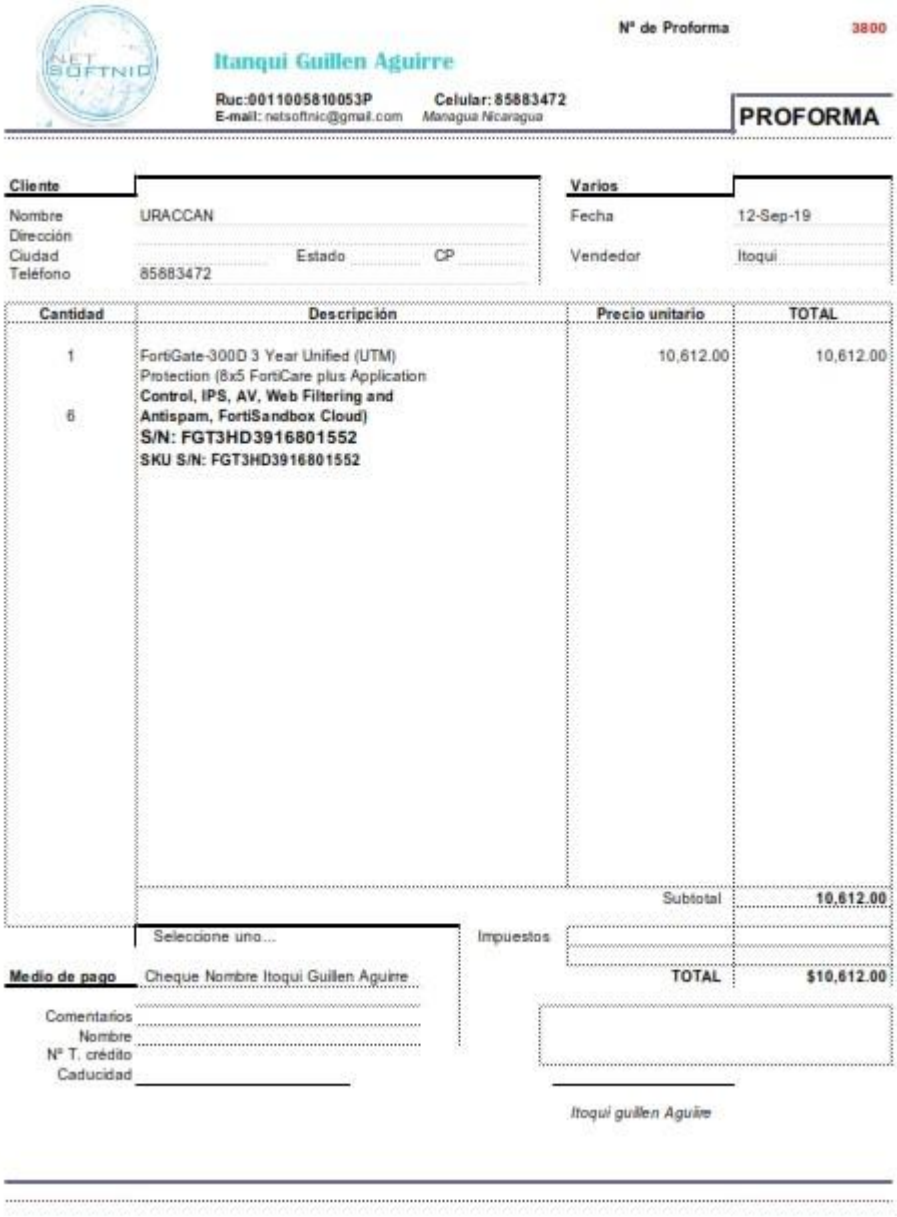
13.3 Comparación de las características de seguridad independientes de los dispositivos UTM de las principales marcas

FUNCIÓN	SOPHOS UTM	SONICWALL NSA	WATCH GUARD XTM	FORTINET Fortigate	Check Point UTM-1
SEGURIDAD BASICA					
Cortafuegos	X	X	X	X	X
Motores Antivirus Simultáneos e independientes	2	1	1	1	1
Protección integrada de estaciones	X	Limitado	Limitado	X	Limitado
TECNOLOGÍAS DE PROTECCIÓN DE ÚLTIMA GENERACIÓN					
Cortafuegos de aplicaciones web	X			X	X
Control de aplicaciones web	X	X	Modelos más grandes	X	X
Sistema de prevención de intrusiones	X	X	X	X	X
Filtrado de datos HTTPS	X	Limitado	Modelos más grandes	Limitado	
CONEXIÓN DE USUARIOS Y OFICINAS REMOTAS					
VPN IPSec y SSL	X	X	Limitado	X	X
Portal VPN	X				
Redes de malla inalámbrica	X			X	X
Portal de autoservicio para usuarios	X			X	
Protección de oficinas remotas lista para usar (RED)	X			X	
FACILIDAD DE USO E IMPLEMENTACIÓN					

Creación predeterminada de informes, para la revisión diaria del rendimiento	X	X	X	X	X
Clúster activo-activo con equilibrio integrado de cargas	X	X	X	X	X
Cuadrante mágico de Gartner de soluciones de UTM	Líder	Líder	Líder	Líder	Líder
LICENCIAS Y SOPORTE					
Conjunto uniforme de funciones en todos los modelos	X	X	X	X	X
Posibilidad de añadir módulos de licencias adicionales según las necesidades	X	X	X	X	Modelos más grandes
Varias opciones de soporte técnico	X	X	X	X	X

Figura 3

13.4 Proforma de UTM Fortinet



Nº de Proforma 3800

Itanqui Guillen Aguirre

Ruc:0011005810053P Celular: 85883472
E-mail: netsoftnic@gmail.com Managua Nicaragua

PROFORMA

Cliente

Nombre URACCAN
Dirección
Ciudad Estado CP
Teléfono 85883472

Varios

Fecha 12-Sep-19
Vendedor Itoqui

Cantidad	Descripción	Precio unitario	TOTAL
1	FortiGate-300D 3 Year Unified (UTM) Protection (8x5 FortiCare plus Application Control, IPS, AV, Web Filtering and Antispam, FortiSandbox Cloud) S/N: FGT3HD3916801552 SKU S/N: FGT3HD3916801552	10,612.00	10,612.00
6			
		Subtotal	10,612.00
	Seleccione uno...	Impuestos	
		TOTAL	$10,612.00

Medio de pago Cheque Nombre Itoqui Guillen Aguirre

Comentarios
Nombre
Nº T. crédito
Caducidad

Itoqui guillen Aguire

Figura 4.

13.5 Oferta solución firewall

SISAP
Sistemas Aplicativos

OFERTA
SOLUCION FIREWALL

FIREWALL SOPHOS XGC210

SISAP
Sistemas Aplicativos

www.sisap.com

Guatemala | El Salvador | Honduras | Costa Rica | Panamá | Nicaragua | República Dominicana

Firewall Sophos XG 210:

Sophos XG Firewall proporciona una protección completa de firewall de última generación que expone los riesgos ocultos, bloquea las amenazas desconocidas y responde automáticamente a los incidentes.

Desempeño y Capacidades

Rendimiento[1]	XG 210 Rev. 3
Rendimiento del firewall	16 Gbps
IMIX del firewall	5,5 Gbps
Rendimiento de la VPN	1,45 Gbps
Rendimiento del IPS	3 Gbps
NGFW (IPS + Control aplic.) máx.	2,9 Gbps
Rendimiento del antivirus (proxy)	2,3 Gbps
Conexiones simultáneas	8.200.000
Conexiones nuevas/seg.	135.000
Número máximo de usuarios con licencia	sin restricciones

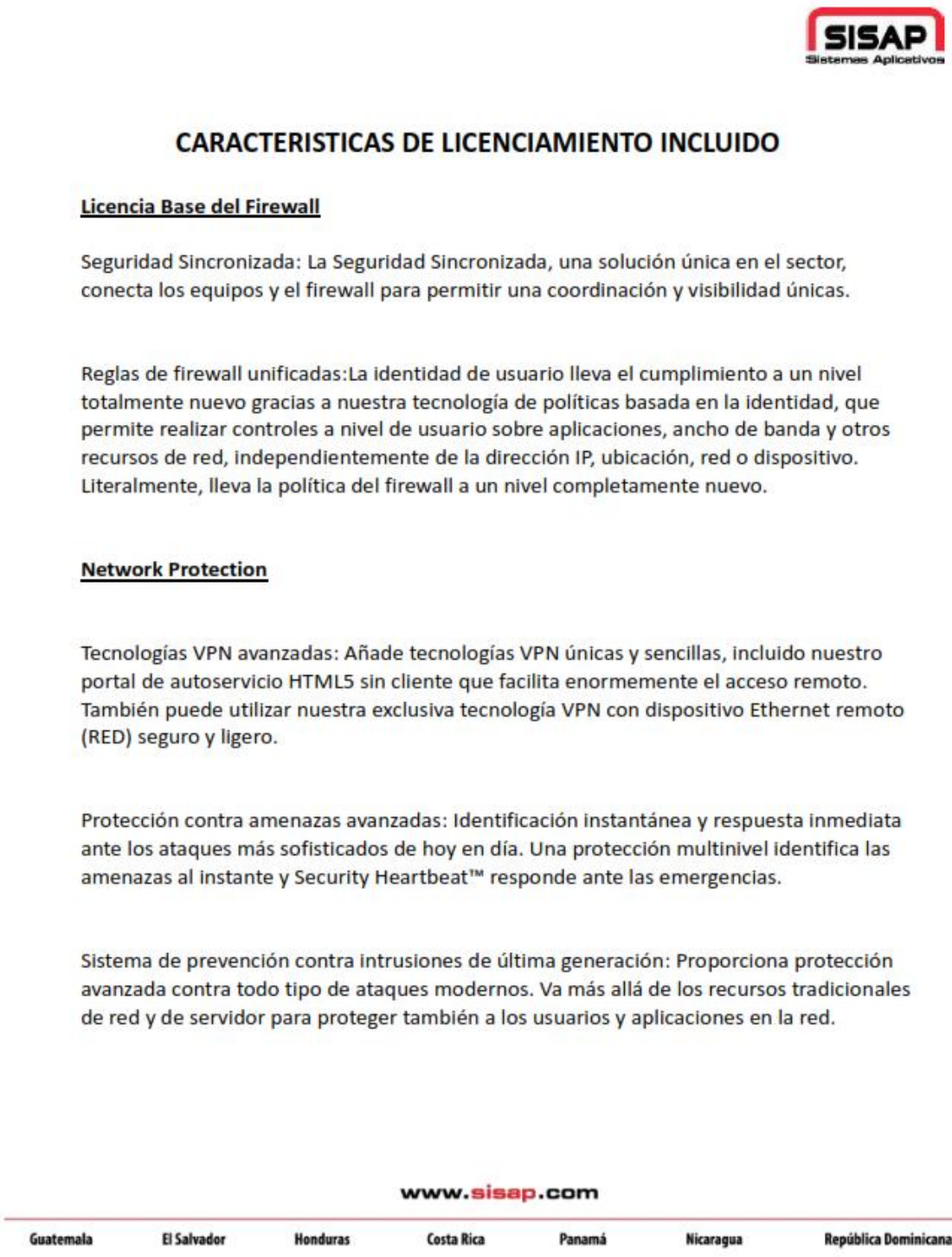
Especificaciones de Hadware

Interfaces físicas	
Almacenamiento (cuarentena local/registros)	SSD integrado
Interfaces Ethernet (fijas)	6 GbE cobre (incl. 2 pares de omisión) 2 GbE SFP
Número de ranuras de puertos FlexiI	1
Módulos de conectividad (opcional)	Módulo DSL SFP (VDSL2) Transceptores SFP/SFP+
Puertos de E/S	2 x USB 3.0 (delantero) 1 x micro USB (delantero) 1 x USB 3.0 (trasero) 1 x COM (RJ45) (delantero) 1 x HDMI (trasero)
Pantalla	Módulo LCD multifunción
Fuente de alimentación	Rango automático interno 100-240 VCA, 50-60 Hz Fuente de alimentación redundante opcional (externa)

www.sisap.com

Guatemala El Salvador Honduras Costa Rica Panamá Nicaragua República Dominicana

Figura 5.



SISAP
Sistemas Aplicativos

CARACTERISTICAS DE LICENCIAMIENTO INCLUIDO

Licencia Base del Firewall

Seguridad Sincronizada: La Seguridad Sincronizada, una solución única en el sector, conecta los equipos y el firewall para permitir una coordinación y visibilidad únicas.

Reglas de firewall unificadas:La identidad de usuario lleva el cumplimiento a un nivel totalmente nuevo gracias a nuestra tecnología de políticas basada en la identidad, que permite realizar controles a nivel de usuario sobre aplicaciones, ancho de banda y otros recursos de red, independientemente de la dirección IP, ubicación, red o dispositivo. Literalmente, lleva la política del firewall a un nivel completamente nuevo.

Network Protection

Tecnologías VPN avanzadas: Añade tecnologías VPN únicas y sencillas, incluido nuestro portal de autoservicio HTML5 sin cliente que facilita enormemente el acceso remoto. También puede utilizar nuestra exclusiva tecnología VPN con dispositivo Ethernet remoto (RED) seguro y ligero.

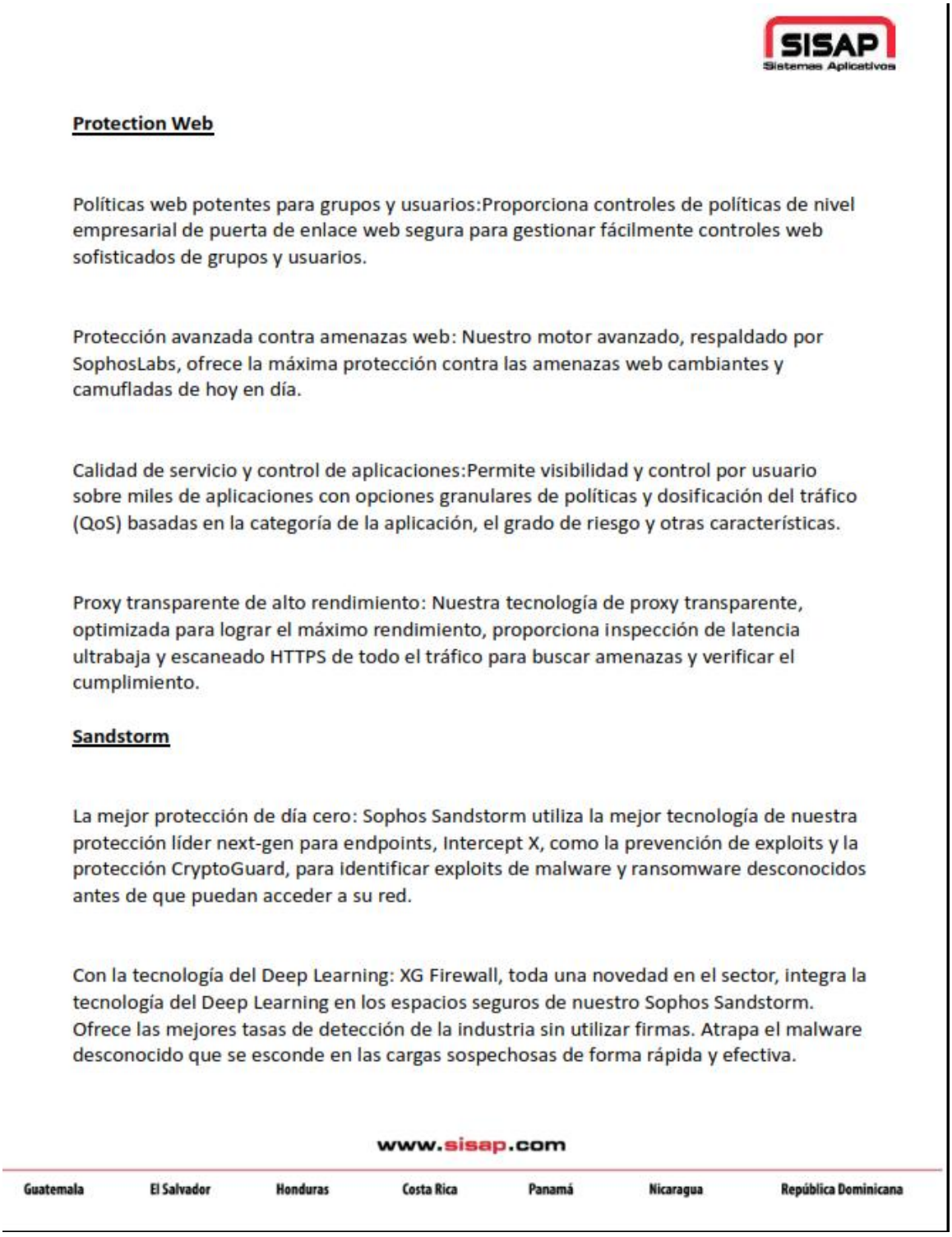
Protección contra amenazas avanzadas: Identificación instantánea y respuesta inmediata ante los ataques más sofisticados de hoy en día. Una protección multinivel identifica las amenazas al instante y Security Heartbeat™ responde ante las emergencias.

Sistema de prevención contra intrusiones de última generación: Proporciona protección avanzada contra todo tipo de ataques modernos. Va más allá de los recursos tradicionales de red y de servidor para proteger también a los usuarios y aplicaciones en la red.

www.sisap.com

Guatemala | El Salvador | Honduras | Costa Rica | Panamá | Nicaragua | República Dominicana

Figura 6.



SISAP
Sistemas Aplicativos

Protection Web

Políticas web potentes para grupos y usuarios:Proporciona controles de políticas de nivel empresarial de puerta de enlace web segura para gestionar fácilmente controles web sofisticados de grupos y usuarios.

Protección avanzada contra amenazas web: Nuestro motor avanzado, respaldado por SophosLabs, ofrece la máxima protección contra las amenazas web cambiantes y camufladas de hoy en día.

Calidad de servicio y control de aplicaciones:Permite visibilidad y control por usuario sobre miles de aplicaciones con opciones granulares de políticas y dosificación del tráfico (QoS) basadas en la categoría de la aplicación, el grado de riesgo y otras características.

Proxy transparente de alto rendimiento: Nuestra tecnología de proxy transparente, optimizada para lograr el máximo rendimiento, proporciona inspección de latencia ultrabaja y escaneado HTTPS de todo el tráfico para buscar amenazas y verificar el cumplimiento.

Sandstorm

La mejor protección de día cero: Sophos Sandstorm utiliza la mejor tecnología de nuestra protección líder next-gen para endpoints, Intercept X, como la prevención de exploits y la protección CryptoGuard, para identificar exploits de malware y ransomware desconocidos antes de que puedan acceder a su red.

Con la tecnología del Deep Learning: XG Firewall, toda una novedad en el sector, integra la tecnología del Deep Learning en los espacios seguros de nuestro Sophos Sandstorm. Ofrece las mejores tasas de detección de la industria sin utilizar firmas. Atrapa el malware desconocido que se esconde en las cargas sospechosas de forma rápida y efectiva.

www.sisap.com

Guatemala | El Salvador | Honduras | Costa Rica | Panamá | Nicaragua | República Dominicana

Figura 7.

13.6 Oferta económica de proveedor

SISAP
Sistemas Aplicativos

OFERTA ECONOMICA

Firewall Sophos XG 210			
Item	Descripcion	Cant.	Precio
1	Equipo Appliance Firewall XG 210 Rev.3 TotalProtect, Licenciamiento Total Protect por 12 meses	1	$7,300.00
2	Licencia Base de Firewall	1	
3	Licencia Network Protection	1	
4	Licencia Web Protection	1	
5	Licencia Sandstorm	1	
6	Implementacion	1	$0.00
7	Soporte tecnico SISAP 7x24, por 12 meses	1	$0.00
		SUB TOTAL:	$7,300.00
		IVA	$1,095.00
		TOTAL	$8,395.00

- Moneda: Dólares de los Estados Unidos de Norteamérica.
- Tiempo de entrega 30 días hábiles

Francisco Centeno
SISAP
O. +505 2255 0600
C. +505 8826 2896 , 505 75152955
francisco.centeno@sisap.com

Figura 8.

13.7 Implementación del proveedor

Elaborado por PROVEEDOR

Fecha: 25 DE Noviembre del 2019

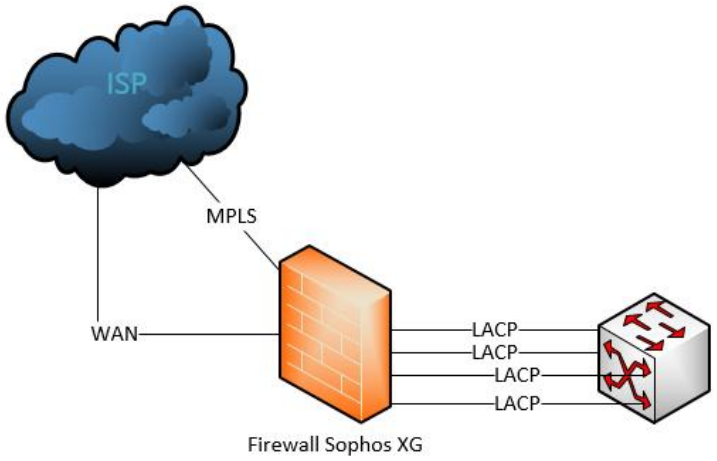
Objetivo

Documentar las configuraciones y pruebas realizadas durante la implementación del firewall Sophos XG, en oficinas de Dirección General de Ingresos de la República de Nicaragua.

Antecedente

La PROVEEDOR realizo la compra del Firewall Sophos XG 210, con el objetivo de implementar sus configuraciones existentes Firewall Sophos XG 210. Información de Configuraciones.

Diagrama Lógico de Solución



Red de Administración

Requisitos	Descripción
Serial	C7434534JJH2423L4
SFOS	ULTIMA VERSION
Hostname	
Dirección IP administración	
DNS1	
DNS2	
NTP	Tiempo. Dominio

Servicios configurados

A continuación, se definen los servicios que se realizaran:

CATEGORÍAS		DETALLE DE SERVICIOS
Servicios de implementación	Montaje	Se realizara el montaje del equipo en el gabinete ubicado en el centro de datos del CLIENTE
	Instalación y configuración	Su configuración y los parámetros iniciales del equipo se actualizarán a la última versión de firmware estable, así mismo la licencia se activo
	Migración	Se realizara las configuraciones en el nuevo equipo. Tomando en cuenta las mejoras presentadas por el nuevo equipo en los módulos implementados.
	Pruebas de funcionalidad	Se realizaran las pruebas de funcionalidad previas a la puesta en producción para validar el correcto funcionamiento de las configuraciones existentes, posteriormente se pasaran a producción.

A continuación se detallan los componentes configurados:

Listado de Tareas
Autenticación
Network Protection
Creación de Reglas de Firewall
IPS
ATP
Web Protection

URL Filtering
Sandstorm
IPS
Application Control
Configuraciones Avanzadas
15 AP Sophos modelos (55 100)
OTP para ingreso a webadmin
VPN Usuario (SSL)
LACP con equipo L3 HP

Nota:

En total se configuraran:

10 redes VLAN, provenientes del LACP.

3 redes Wireless.

1 Hotspot.

8 interfaces físicas.

18 zonas de seguridad.

370 objetos IP.

145 objetos de grupos IP.

30 Servicios.

19 rutas estáticas.

270 reglas de Firewall.

90 VPN

13.8 Oferta economica del proveedor

Fecha: 14/01/2019
Oferta: MROB-PAN850.DGI.002.V1
Pagina - 1

OFERTA ECONOMICA

Cliente: DIRECCION GENERAL DE INGRESOS
Atención: **Jose Herrea**

Dirección: Contiguo a Pizza Hut Villa Fontana
Edificio CAR III, tercer piso.

RUC J0110000014087

ITEM		NO. DE PARTE	DESCRIPCION	CANTIDAD	PRECIO UNITARIO	PRECIO EXTENDIDO
		Productos				
1,0	**PALO ALTO NETWORKS FIREWALL & URL**	PAN-PA-850	Palo Alto Networks PA-850	4	$11.800,00	$47.200,00
		Soportes y Equivalentes, con opción a renovaciones anuales (Equivale a 2 años)				
1.0.1		PAN-PA-850-URL4-HA2	PANDB URL filtering subscription for device in an HA pair year 1, PA-850	4	$1.890,91	$7.563,64
1.0.2		PAN-PA-850-TP-HA2	Threat prevention subscription for device in an HA pair year 1, PA-850	4	$1.890,91	$7.563,64
1.0.3		PAN-PA-850-WF-HA2	WildFire subscription year 1 for device in HA pair, PA-850	4	$1.890,91	$7.563,64
1.0.4		PAN-SVC-PREM-850	Premium support 1-year prepaid, PA-850	4	$2.704,55	$10.818,18
		Servicios Profesionales				
2,0			**Servicios profecionales incluyen:** 1. Instalación y configuración, PA 850. Servicios de Instalacion y Configuracion de 4 Equipos PA-850 en HA./ 2 en DGI Managua 2 en DGI Leon. Transferencia de Conocimiento. De lo configurado y Tareas diarias. Configuracion del SLR (security Life cycle Review). 1 visita por semana durante 2 meses. 2. Capacitacion en idioma español Impartida por SPC Internacional.	1	$2.000,00	$2.000,00

SUB-TOTAL (SIN IVA)	**$82.709,09**
IVA	**$12.406,36**
TOTAL	**$95.115,45**

Tiempo de entrega: 30-45 días, sujeto a cambios de fabrica o leyes del pais de origen.

Vigencia de la oferta: 30 dias.
Garantía de extendida del fabricante renovables por un año.

Condiciones de pago: 60 % contra Orden de Compra y 40% contra entrega de equipos.

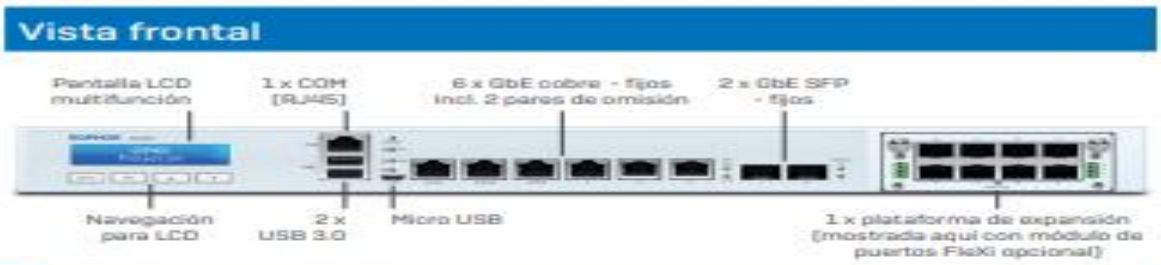
Muy Cordialmente,

Maria Renee Orozco
morozco@spcinternacional.com
Consultor de Negocios - SPC Internacional
Celular.: +505 82383289
PBX.: +505 22998425 ext.1208

13.9 Características técnicas de Sophos UTM XG 210

Los dispositivos XG 210 de Sophos están diseñados para proteger a organizaciones grandes y pequeñas hasta las sucursales. Basados en la última tecnología de Intel y equipados con 6 puertos GbE de cobre, 2 puertos de fibra GbE SFP y una ranura FleXi Port para configurarse con un módulo opcional, proporcionan una gran flexibilidad y velocidad con una excelente relación entre precio y rendimiento. Existe la opción de una fuente de alimentación redundante externa para estos modelos.

Figura 9.



Entorno	
Consumo de energía	XG 210: 19W, 65 BTU/h (inactivo) 35W, 119 BTU/h (carga completa) XG 230: 21W, 72 BTU/h (inactivo) 41W, 141 BTU/h (carga completa)
Temperatura en funcionamiento	0-40°C (en funcionamiento) -20 a +80°C (almacenamiento)
Humedad	10%-90%, sin condensación

Certificaciones de productos	
Certificaciones	CB, UL, CE, FCC Clase A, ISED, VCCI, RCM, CCC, KC, BIS

Figura 10.

Rendimiento[1]	XG 210 Rev. 3
Rendimiento del firewall	16 Gbps
IMIX del firewall	5,5 Gbps
Rendimiento de la VPN	1,45 Gbps
Rendimiento del IPS	3 Gbps
NGFW (IPS + Control aplic.) máx.	2,9 Gbps
Rendimiento del antivirus (proxy)	2,3 Gbps
Conexiones simultáneas	8.200.000
Conexiones nuevas/seg.	135.000
Número máximo de usuarios con licencia	sin restricciones

Figura 11.

Interfaces físicas	
Almacenamiento (cuarentena local/registros)	SSD integrado
Interfaces Ethernet (fijas)	6 GbE cobre (incl. 2 pares de omisión) 2 GbE SFP*
Número de ranuras de puertos FleXi	1
Módulos de puertos FleXi (opcional)	GbE cobre de 8 puertos GbE SFP de 8 puertos* 2 puertos de 10 GbE SFP+* 4 puertos de 10 GbE SFP+* 2 puertos de 40 GbE QSFP+* PoE GbE de 4 puertos PoE GbE de 8 puertos GE cobre de 4 puertos con omisión LAN
Módulos de conectividad (opcional)	Módulo DSL SFP (VDSL2) Transceptores SFP/SFP+
Puertos de E/S	2 x USB 3.0 (delantero) 1 x micro USB (delantero) 1 x USB 3.0 (trasero) 1 x COM (RJ45) (delantero) 1 x HDMI (trasero)
Pantalla	Módulo LCD multifunción
Fuente de alimentación	Rango automático interno 100-240 VCA, 50-60 Hz Fuente de alimentación redundante opcional (externa)
Especificaciones físicas	
Montaje	Montaje en bastidor 1U (2 orejas de montaje en bastidor incluidas)
Dimensiones Ancho x Profundidad x Altura	438 x 344,4 x 44 mm 17,24 x 13,56 x 1,75 pulgadas
Peso	5,2 kg / 11,46 lbs (fuera del paquete) 7,7 kg / 16,98 lbs (en el paquete)